FAKULTÄT FÜR !NFORMATIK
Faculty of Informatics

# International police data exchange from a technical, organisational and legal point of view

DIPLOMA THESIS

submitted in partial fulfillment of the requirements for the degree of

**Diplom-Ingenieur**

in

**Business Informatics**

by

**David Melcher BSc**
Registration Number 0651252

to the Faculty of Informatics

at the Vienna University of Technology

Advisor: Ao. Univ.-Prof. Mag. Dr. iur. Markus Haslinger

Vienna, 2nd April, 2020

David Melcher

Markus Haslinger

Technische Universität Wien
A-1040 Wien ▪ Karlsplatz 13 ▪ Tel. +43-1-58801-0 ▪ www.tuwien.ac.at

# Erklärung zur Verfassung der Arbeit

David Melcher BSc
Webgasse 12/08
1060 Wien

Hiermit erkläre ich, dass ich diese Arbeit selbständig verfasst habe, dass ich die verwendeten Quellen und Hilfsmittel vollständig angegeben habe und dass ich die Stellen der Arbeit – einschließlich Tabellen, Karten und Abbildungen –, die anderen Werken oder dem Internet im Wortlaut oder dem Sinn nach entnommen sind, auf jeden Fall unter Angabe der Quelle als Entlehnung kenntlich gemacht habe.

Wien, 2. April 2020

David Melcher

# Danksagung

An dieser Stelle möchte ich mich bei all denjenigen bedanken, die mich während der Anfertigung dieser Diplomarbeit unterstützt und motiviert haben.

Zuerst gebührt mein Dank Herrn Ao. Univ.-Prof. Dr. iur. Markus Haslinger, der meine Diplomarbeit betreut und begutachtet hat. Für die hilfreichen Anregungen und die konstruktive Kritik bei der Erstellung dieser Arbeit möchte ich mich herzlich bedanken.

Ein besonderer Dank gilt den InterviewpartnerInnen, die ihr fachliches Wissen mit mir geteilt haben.

Mein Dank geht auch an Dr. Josef Prüger für seine stete Bereitschaft zu kritischen Diskussionen, für seine motivierenden Anregungen zum Fertigwerden meiner Arbeit.

Außerdem möchte ich Marion Janschitz, MSc für das Korrekturlesen meiner Masterarbeit danken.

Besonders bedanke ich mich bei meiner Schwester Dipl.-Ing. Sophia Melcher und ihrem Partner Dr. Elias Aschauer, die mich besonders in der Endphase der Arbeit motiviert haben. Sie waren immer meine Ansprechpartner und standen mir mit gutem Rat zur Seite.

Ebenfalls danke ich meinen Mitbewohnern Andreas der mit seinem scharfen Auge mich auf Feinheiten aufmerksam machte und Fritz, die immer ein offenes Ohr für mich haben und mich stets mit spannenden und hitzigen Diskussionen unterhalten.

Abschließend möchte ich mich bei meinen Eltern Dipl.-Päd. Veronika und Dipl.-Ing. Dan Melcher bedanken, die mir mein Studium durch ihre Unterstützung ermöglicht haben.

# Kurzfassung

Organisierte Schwerkriminalität, wie beispielsweise Drogen-, Waffen- und Menschenhandel, aber auch Produktpiraterie, Geldwäsche und im weitesten Sinne Terrorismus, hat durch die rasante wirtschaftliche Globalisierung der letzten Jahrzehnte strukturelle Veränderungen und andere Entwicklungen erfahren, mit denen einzelstaatliche Polizeibehörden immer weniger Schritt halten können.

Erfolge zur Prävention und Bekämpfung grenzüberschreitender Schwerkriminalität können daher nur durch Kooperation zwischen den Polizeibehörden und einen internationalen Polizeidatenaustausch erzielt werden. Das Prinzip ist hierbei die Akkumulation ungeheurer Datenmengen als Basis für umfassende internationale Analyse, Auswertung und Informationsbeschaffung zur Verhinderung von Delikten und erfolgreicher Verfolgung von Straftätern.

Ein solcher Datenaustausch stellt eine Herausforderung auf legaler, organisatorischer, semantischer und technischer Ebene dar. Es müssen nicht nur die verschiedenen Prozesse und Systeme interoperabel gemacht werden, sondern auch der Umgang mit den technologischen und administrativen Möglichkeiten muss einem internationalen Konsens und konkreten Richtlinien unterworfen werden.

Neben den positiven Sicherheitsaspekten solcher Polizeikooperationen gilt es aber auch die sich aus dieser Datenfülle möglicherweise ergebenden Probleme zu beleuchten. Das oberste Gebot ist in diesem Fall der Datenschutz und die Datensicherheit, um zu verhindern, dass BürgerInnen zu „gläsernen Menschen“ werden.

# Abstract

Due to rapid economic globalisation within the last decades, organised criminal activities like drug-, weapon-, and human trafficking, as well as product piracy, money laundering and by extension terrorism, have gone through structural changes and experienced developments that national police authorities are increasingly unable to keep up with.

Effective prevention and control of transnational organised crime requires cooperation between authorities and therefore international police data exchange. The objective is to accumulate enormous amounts of data as a fundament for comprehensive international analysis, interpretation and information procurement in order to avert delicts and prosecute criminals successfully.

This quantity of data exchange poses a challenge on legal, organisational, semantic and technical levels. Not only differential processes and systems warrant increased interoperability, it is also necessary to provide international consensus and to agree on distinct guidelines regarding the handling of technologies and administrational opportunities.

Although the positive aspects of police cooperation are evident, this wealth in data might also harbour problems that have to be addressed. First and foremost, data protection and security have to be guaranteed to prevent citizens from turning into “vitreous humans”.

# Contents

**Kurzfassung** **vii**

**Abstract** **ix**

**Contents** **xi**

**1 Introduction** **1**
1.1 Problem Statement . . . . . 1
1.2 Structure and Scope of this Work . . . . . 2

**2 Concepts and Limitations of Police Cooperation** **3**
2.1 Theoretical Foundations of Police Cooperation . . . . . 3
2.1.1 Terminology . . . . . 3
2.1.1.1 Interoperability . . . . . 4
2.1.1.2 Police Cooperation . . . . . 4
2.1.1.3 Organised Crime . . . . . 5
2.1.2 Underlying International Relations Concepts . . . . . 5
2.1.2.1 Supranationalism . . . . . 6
2.1.2.2 Intergovernmentalism . . . . . 6
2.1.2.3 Multi-Level-Governance . . . . . 6
2.1.3 Limiting Legal and Administrative Impediments . . . . . 6
2.1.3.1 Constitutional Systems . . . . . 7
2.1.3.2 Sovereignty of Nation States . . . . . 7
2.1.3.3 Inhomogeneity of Police Structures . . . . . 8
2.2 Public Administration Approaches in the Digital Age . . . . . 9
2.2.1 Overview of Forms and Function of e-Government . . . . . 9
2.2.2 European Interoperability Framework . . . . . 10

**3 Global, European and Austrian Police Cooperation** **13**
3.1 Europeanisation of Police Cooperation . . . . . 13
3.1.1 TREVI Cooperation . . . . . 14
3.1.2 The Single European Act . . . . . 15
3.1.3 Schengen Agreement . . . . . 16
3.1.4 Treaty of Maastricht . . . . . 18

3.1.5 Treaty of Amsterdam . . . 19
3.1.6 Treaty of Nice . . . 20
3.1.7 Treaty of Lisbon . . . 21
3.1.8 Prüm Decisions . . . 22
3.2 Police and Judicial Authorities . . . 23
3.2.1 Interpol . . . 24
3.2.1.1 History of Interpol . . . 24
3.2.1.2 Area of Responsibility . . . 26
3.2.2 Europol . . . 27
3.2.2.1 History of Europol . . . 28
3.2.2.2 Legal Status and Organisation . . . 30
3.2.2.3 Operation and Responsibility . . . 32
3.2.2.4 International Position in Criminal Prosecution . . . 33
3.2.2.5 Exemplary Relevant Figures . . . 34
3.2.3 Eurojust . . . 35
3.2.3.1 History of Eurojust . . . 35
3.2.3.2 Structure and Organisation . . . 36
3.2.3.3 Areas of Responsibility and Legal Status . . . 36
3.2.4 The European Court of Justice . . . 38
3.2.5 The Austrian Federal Police . . . 39
3.2.5.1 The Federal Criminal Police Office . . . 39

**4 Data Protection Law** **43**
4.1 A Brief History of Data Protection . . . 43
4.2 European Digital Single Market . . . 45
4.2.1 Digital Economy . . . 46
4.2.2 Strategy Objectives . . . 47
4.2.3 ePrivacy Regulation . . . 48
4.2.4 European Data Protection Supervisor . . . 48
4.3 General Data Protection Regulation . . . 49
4.3.1 Structure . . . 49
4.3.2 Aims and Principles . . . 50
4.3.3 Rights of the Data Subject . . . 51
4.3.4 Liability and Penalties . . . 53
4.4 Data Protection Law and Europol . . . 54

**5 Interoperability** **57**
5.1 European Interoperability Framework . . . 57
5.1.1 Underlying Principles of European Public Services . . . 60
5.1.2 Conceptual Model for Integrated Public Service Provision . . . 61
5.1.3 Interoperability Layers . . . 63
5.1.3.1 Legal Interoperability . . . 63
5.1.3.2 Organisational Interoperability . . . 64
5.1.3.3 Semantic Interoperability . . . 65

5.1.3.4 Technical Interoperability . . . . . 65
5.1.3.5 Interoperability Governance . . . . . 66
5.2 Database Cross-linking . . . . . 67

**6 Methodology of Police Data Exchange 71**
6.1 Data Structures and Communication Systems . . . . . 71
6.1.1 XML Data Format . . . . . 71
6.1.2 Universal Message Format (UMF) . . . . . 72
6.1.3 Reference Model POLICE . . . . . 74
6.1.4 Excursion: Digital Austria . . . . . 75
6.2 European and Austrian Police Information Systems . . . . . 77
6.2.1 Europol Information System (EIS) . . . . . 78
6.2.2 Europol Analysis System (EAS) . . . . . 79
6.2.3 Secure Information Exchange Network Application (SIENA) . . 81
6.2.4 Schengen Information Systems (SIS) . . . . . 83
6.2.5 Europol Platform for Experts (EPE) . . . . . 84
6.2.6 Austrian Police Information Systems . . . . . 85
6.2.6.1 "Integriertes Polizeiliches Sicherheitssystem" (IPOS) . . 86
6.2.6.2 IKDA, PAD and ZDS . . . . . 86
6.2.6.3 Security Monitor . . . . . 87
6.2.6.4 "Factotum" Databases . . . . . 87

**7 Impact and Success of European Police Cooperation 89**
7.1 Select efforts of European Police Cooperation . . . . . 89
7.1.1 European Crime Prevention Network . . . . . 90
7.1.2 Joint Investigation Teams . . . . . 90
7.1.3 EMPACT Platform . . . . . 91
7.2 Police Cooperation with and within Austria . . . . . 94
7.2.1 European Impact on Austrian Police Administration . . . . . 94
7.2.1.1 Crime Prevention . . . . . 94
7.2.1.2 European Police Cooperation Act . . . . . 95
7.2.1.3 Internal Security and Criminal Prosecution . . . . . 96
7.2.2 Excursion: .BK Audit Report 2015 . . . . . 97

**8 Conclusion 101**

**List of Figures 103**

**Bibliography 111**

CHAPTER 1

# Introduction

## 1.1 Problem Statement

In the light of Europe's political coalescence to form the European Union (EU) as an Area of Freedom, Security and Justice (AFSJ), international and intranational police cooperation between authorities of the EU and individual EU member states is of crucial importance.

The high degree of heterogeneity within the EU regarding political, legal, organisational and cultural characteristics of member states, however, poses a great challenge to overcome and establish seamless police cooperation on a European level. In addition to hindrances due to these national differences, technical aspects have to be kept in mind. The creation of interfaces between the systems used by national authorities requires standardisation and harmonisation of technological resources and procedures. Lastly, electronic and digital applications and technologies are increasingly ubiquitous in public administration and the governmental sector. While posing an enormous amount of opportunities to exploit the potential of high-throughput information and data exchange as means for increased productivity in all sectors, this gigantic increase in available information also requires appropriate management and sensible handling. The rapid developments in the Information and Communication Technology (ICT) sector emphasise the necessity of a high level of digital awareness when planning, organising and performing administrational and executional operations, including those of the sector of security and justice.

Therefore, my thesis can be seen as a review of international police cooperation, discussing these three points:

1. The early political approaches to promote international police coordination and the result of the emergence of the EU on their development.

2. The legal, organisational and technical requirements for international police cooperation and their implementation.

3. The current successes and deficits of police cooperation and future plans.

## 1.2 Structure and Scope of this Work

This work discusses the efforts, developments and results of global international police cooperation. It focusses on the cooperation in Europe and the European Union and shows its impact on Austria.

The thesis is structured in a way that enables readers to first build a general knowledge on police cooperation and the political background of the EU, followed by a more in-depth discussion of specific aspects of international developments and approaches. Still, each chapter can be seen as an individual unit. As different aspects are interconnected and built on a similar background, overlaps and repetitions are intentional.

Chapter 2 introduces important terminology and basic concepts of police cooperation. Furthermore, it sheds a first light on existing European structures.

Chapter 3 first gives an extensive overview of the evolution of the European Union, focusing on its implications in law enforcement and justice. The second part of this chapter presents and discusses important police and judicial authorities on the global, European and Austrian level. These authorities are Interpol, Europol, Eurojust, the European Council and the Austrian Federal Police with the Federal Criminal Police Office ("Bundeskriminalamt", .BK) as operational centerpiece.

Chapter 4 addresses the major problem that comes with the electronic concatenation of information systems and data exchange, namely data protection and security. It discusses current regulations and illustrates limitations in the light of EU's paragon position regarding these aspects.

Chapter 5 focuses on the concept of interoperability, an essential parameter of efficient and effective cooperation between international authorities of all sectors. The legal, organisational, semantic and technical aspects of interoperability are introduced as they constitute the vital foundation for any kind of international relation.

Chapter 6 provides information on the methodological and predominantly technical possibilities and limitations of police data exchange. It introduces data format standards, provides an overview of existing information systems in Europe and Austria and displays the current technological situation.

Chapter 7 serves as a review of the current successes of European police cooperation and discusses the impact of Europeanisation of Austrian politics in the area of law enforcement.

CHAPTER 2

# Concepts and Limitations of Police Cooperation

The aim of international police data exchange is to provide interoperability of border-crossing collaborations to prevent and effectively control organised crime. This chapter comprises a description of the theoretical basics of police collaboration in the European cooperation process, defines relevant terminology and addresses the role of an ICT-framework in respect of European interoperability.

## 2.1 Theoretical Foundations of Police Cooperation

Police collaboration on European level is based on a blend of defined concepts of international law which define their international relations.

National police authority (and the success of international and intranational police work) is directly dependent on contextual and administrational consensus between the respective political levels and entities. Differences in these regards affect the executability and degree of interoperability of police collaboration.

### 2.1.1 Terminology

The prerequisite for international police data exchange is cross-border police cooperation. Effective police cooperation is only possible if - despite a given range of barriers (such as different languages, different mentalities and cultural standards, different organisations, different file formats or different programs) a consensus for a uniform approach can be agreed upon. An established procedure that is comprehensible, reasonable and applicable for all participants can be explicitly described as interoperability.

Hereafter, the relevant terms interoperability, police cooperation and organised crime are addressed in detail.

#### 2.1.1.1 Interoperability

The European Parliament and of the Council defines interoperability as "the ability of disparate and diverse organisations to interact towards mutually beneficial and agreed common goals, involving the sharing of information and knowledge between the organisations, through the business processes they support, by means of the exchange of data between their respective ICT systems".[1]

Software is particularly considered interoperable if several programs use the same file format and protocols.[2]

To assist describing the term comprehensibly, one can consult three additional definitions which are analogous in their interpretation:

1. Interoperability is the ability of various systems to work together seamlessly.[3]

2. Interoperability designates the collaboration ability of different systems, techniques or organisations while adhering to common standards.[4]

3. Interoperability is the ability of independent heterogenic systems to collaborate seamlessly with the aim of efficient information exchange. The results are provided to users without the necessity of separate agreements between the systems.[5]

Interoperability is essential in informatics, telecommunication, medical technologies, transport and traffic systems, military systems, industrial automation technologies, and e-government.

#### 2.1.1.2 Police Cooperation

Police collaboration can be discussed on the national, bilateral, European and international level.

On a national level, it is defined as the collaboration between the federal police, the national police headquarters and the special forces of the ministry of internal affairs. The collaboration between Austrian and German law enforcement authorities is an example of bilateral police cooperation. The European level of police collaboration is carried out between the Federal Criminal Police Office and Europol. On an international level, one can find collaboration between the Federal Criminal Police Office and Interpol.

[1] [PotC09] - Decision No 922/2009/EC - Art. 2 (a).
[2] [Enc18]
[3] [Dud] - cf. Duden: "Fähigkeit unterschiedlicher Systeme, möglichst nahtlos zusammenzuarbeiten."
[4] [Wik19]
[5] ibid.

The aim of this cooperation is to establish Europe as an Area of Freedom, Security and Justice (AFSJ)[6], where basic civil rights are consistently valued. Effective, cross-border police collaboration in the process of criminal prosecution is a key element in the prevention and investigation of criminal offences. To achieve this, a combined effort by police, customs, and other authorities, mainly aiming at serious crime (organised crime, drug trafficking, human trafficking, internet criminality) and terrorism is made.[7]

#### 2.1.1.3 Organised Crime

Organised crime is a constructed term, a general definition is lacking.[8] Nevertheless, there exist these three basic assumptions regarding the nature of organised crime:[9]

1. It is a specialised category of criminal conduct, namely the "profit- or power-dominated, methodical commission of crimes".[10]

2. The crime itself is not necessarily organised, but the criminals are. Organised crime, therefore, relates to organised criminal groups with a hierarchical structure.[11]

3. The central circumstance of organised crime is the exertion of power. If this happens within an alliance of criminal and societal elites, it is referred to as "extra-legal governance"[12]. In this case, one deals with the regulation of social structures that are not regulated by the state due to lack of interest or ability. Black markets or criminal milieus are examples of this. Here, organised crime also describes the corruption of the constitutional order in the form of a collaboration between criminal communities, economy, and politics.[13]

### 2.1.2 Underlying International Relations Concepts

Three theories in political science that are in parts strongly associated with the EU are supranationalism, intergovernmentalism and multi-level-governance.[14] Taken together, these concepts of international law comprise the foundations of European police cooperation

[6] [Uni12b] - Article 3 (2) TEU (Treaty on European Union) "The Union shall offer its citizens an area of freedom, security and justice without internal frontiers, in which the free movement of persons is ensured in conjunction with appropriate measures with respect to external border controls, asylum, immigration and the prevention and combating of crime."

[7] [Kri18]

[8] [vL13]

[9] ibid.

[10] ibid. - "Gewinn- oder Machtstreben bestimmte planmäßige Begehung von Straftaten" - Bundeslagebild organisierte Kriminalität 2011 - September 14th 2012, p. 10.

[11] ibid. - Definition of the FBI.

[12] ibid. - [Cam11, p. 224]

[13] ibid.

[14] [Sch12, p. 17f.]

#### 2.1.2.1 Supranationalism

Surpranationalism describes a multinational political union where political authority is exerted by the governments of member states. The term supranational union is related to the European Union:[15]

"Europe is a Europe of free, independent sovereign nations who choose to pool that sovereignty in pursuit of their own interests and the common good, achieving more together than we can achieve alone. The EU will remain a unique combination of the intergovernmental and the supranational."[16]

#### 2.1.2.2 Intergovernmentalism

The term intergovernmentalism can – in the context of international and European law - be interpreted as the collaboration of states within the framework of internationally operating organisations. Examples for applied intergovernmentalism are the United States and parts of the European Union. In these cases, the Common Foreign and Security Policy (CFSP) is part of intergovernmental cooperation: By applying the principle of unanimity (right of veto) the discretionary competence is ensured for each state.[17]

#### 2.1.2.3 Multi-Level-Governance

The multi-level-governance approach can be understood as applied institutionalism. It refers to the interaction between different governmental levels when dealing with management-related and regulatory tasks.

With this model, the concept of a central governing and executing entity is expanded by several governmental levels with different competences that take on tasks within political fields where they command the respective best-fitting resources.

This approach is therefore as such comparable with the principle of subsidiarity, meaning that decision finding processes should be initiated on a citizen-oriented level.

Multi-level-governance as vertical political integration is an endeavour to establish cooperation and consensus of the various given levels. It is crucial to define precise rules for shared competences.[18]

### 2.1.3 Limiting Legal and Administrative Impediments

Besides contextual differences and problems that arise from divergent jurisdiction standards within the EU, existing deficits in the administrational sector impede efficient police cooperation as well.

[15] [Kil04, p. 21]
[16] [BBPC10] - Tony Blair, British Prime Minister: Polish Stock Exchange (Warsaw, October 6th 2000).
[17] [Jon14]
[18] [Hüt14]

#### 2.1.3.1 Constitutional Systems

The prime obstacle for efficient police collaboration are "various legal and constitutional traditions of the member states as regards police powers, gathering of personal data at national level and data protection.".[19] The ideal of a so-called multi-speed Europe – where integration is established at different paces according to the political situation of individual nations – results in heterogeneity regarding civic protection and the Area of Freedom, Security and Justice.[20]

#### 2.1.3.2 Sovereignty of Nation States

National sovereignty - nation's supreme authority of autonomous self-government - is the key element when it comes to international security, criminal prosecution an jurisdiction. Reassigning related duties to a supranational player or an international organisation is hardly conceivable. Sovereignty is repeatedly discussed in the EU since many nations strongly oppose the loss of sovereignty, especially regarding the Europeanisation of police work. However, the national states acknowledge the futility of trying to control new crime forms on their own. Transnational crime and illegal migration nevertheless show the necessity of international consensus.

An additional problem when Europeanising internal security is the enforcement of the member states' national interests. Before the Treaty of Lisbon[21] was brought into action, a veto against decisions in the areas of domestic and juridical politics put in by any of the Union's member states could bring a negotiation process to a complete standstill.

With the Treaty of Lisbon, however, the power of ultimate decision regarding judicial police collaboration in criminal affairs was conveyed to the first of three supranational pillars of the European Union.

Still, a non-participation in specific EU projects can be granted to individual member states in the form of exclusion clauses that have been adopted as an "opt-out"-mechanism.[22]

These exclusion clauses are often used to elude compulsory implementation commitment. They promise flexibility, supposedly contributing to accelerated integration processes. In reality, however, exclusion clauses hamper efforts to assimilate divergent police work standards significantly.[23]

[19] [tCoCLJA09, p. 3]
[20] ibid.
[21] [bUUoL19g]
[22] [KP08, p. 8] - Kietz and Parkes 2008.
[23] [JKK06, p. 27] - Jachtenfuchs and Kohler-Koch 2006.

#### 2.1.3.3 Inhomogeneity of Police Structures

Even experts face difficulties when attempting to keep an overview of all existing forms of bi- and multilateral police collaborations in Europe.[24] Of course, this generates the risk of parallel development, overlaps, contrary results and therefore excess work.

A divergent police culture that abides by different traditions additional becomes very evident in matters of applied technologies and working procedures within police institutions. Cultural exchange, however, has been made available with the establishment of Europol, mainly due to the common positioning of liaison officers in a single building, thus facilitating access to information shared amongst member states. Additional approaches focus on the joint education according to European standards, as offered by the European Police College (Collège Européen de Police, CEPOL),[25] aiming for the following objectives:[26]

- Harmonisation of content and structure of national general and advanced education.
- European educational standards that convey a strong understanding of basic rights and rights of freedom.
- Coordination and promotion of advanced education for experts and faculty members.
- A regular and consistent exchange of professors and students attending national police academies.
- Mutual approval of academical degrees from national teaching facilities.

Besides governmental efforts to unify police work standards, a valuable asset to reduce potential international differences and disagreements could of course also be found in associations that are often made possible by non-governmental organisations. Involving colleagues directly by giving them opportunities for trans-European networking consequentially leads to a better starting point for congruent decision making, which also positively affects technological information exchange and therefore IT-based interoperability.

Noteworthy associations are the International Police Association (IPA)[27] as the world's largest police association that has been established in the 1950s, and, on a European level, the European Police Association (EPA), which was founded in 1995.[28] Additionally, communication and collaboration within specialised police branches are supported across the EU by associations like the European Association of Railway Police Forces (RAILPOL)[29] or the European Network of Policewomen (ENP)[30].

[24] [Feh09, p. 2] - Fehérváry 2009.
[25] [PotC15] - Regulation (EU) 2015/2219.
[26] [Uni16b]
[27] [IPA19]
[28] [Ass19]
[29] [RAI19]
[30] [ENP19]

## 2.2 Public Administration Approaches in the Digital Age

In the age of omnipresent, internet-supported, electronic communication that is even discussed as a significant factor of socioeconomic progress in developmental countries,[31] it does not come as a surprise that administration, execution, and regulation of international and intranational public affairs are increasingly digitalised, a development, which is condensed in the term e-Government.[32] The establishment of e-Government Interoperability Frameworks (eGIFs) is essential to combine highly diverse fields of accountability and execution within public services smoothly. This necessitates the integration of several aspects or layers of interoperability to ensure efficient intranational and international collaboration.

### 2.2.1 Overview of Forms and Function of e-Government

The term e-Government essentially describes the usage of information technology (IT) in national affairs. However, it does not only comprise IT-based application in governmental processes but extends to the digitalisation of information exchange, communication between instances or individuals, public services and the integration of independent systems.[33]

The different forms of e-Government are:[34]

- G2C (government-to-citizen): Digital services are provided to citizens aiming at improved and simplified relations between the state and citizen. Relevant European examples are the implementation of digital signatures and biometric passports.
- G2E (government-to-employees): Communication and interaction between employers, employees and the government are facilitated by measures like the digitalisation of labour law-related documents (personal data, payslips, insurance, tax return) or e-learning.
- G2B (government-to-business): Interactions between the government and businesses that provide corporate consulting on a non-commercial basis as well as easier online business processing are in focus.
- G2G (government-to-government): These are tasks in the fields of integration, communication, and organisation of international affairs. For international public services, this form of e-government is essential for interoperability on several levels.

[31] [Mad00] - Madon 2000.
[32] [PS07] - Palvia and Sharma 2007.
[33] [HJ07] - Hai and Jeong 2007.
[34] [ES17]

### 2.2.2 European Interoperability Framework

An Interoperability Framework differs from pure technical interoperability by including application guidelines and clearly stated standards when dealing with existing technologies.

An e-Government Interoperability Framework is described as "a document or group of documents that specify a set of common elements such as vocabularies, concepts, principles, policies, guidelines, recommendations, standards, and practices for agencies that wish to work together, towards the joint delivery of public services".[35] It is established to standardise and therefore facilitate governmental processes on the regional, national and international level.

A whole range of standardisation processes in the EU is regulated by the European Interoperability Framework (EIF). The first draft of the EIF was already published through the Interoperable Delivery of European eGovernment Services to public Administrations, Businesses and Citizens (IDABC) program in 2004.[36] It was revised in 2010[37] and recommended 25 measures[38] that were then supported by the ISA program (Interoperability Solutions for European Public Administrations, Businesses and Citizens).[39]

After an update in 2016, the newest version of the EIF[40] was developed within the scope of the European e-government action plan 2016-2020 (strategy for the digital domestic market) and implemented in 2017 using the ISA$^2$ program.[41] The new EIF comprises 47 recommendations and is divided into three main points:[42]

- The underlying principles for European services - The principles of the EIF constitute recommendations regarding the member states' subsidiarity, core principles that serve as a prerequisite for the functioning of the framework. These principles address the users' needs and establishes guidelines regarding the operational aspects of transnational cooperation directly.
- The conceptual model for public services - The conceptual model of the EIF promotes combining individual service components with base registry data to create complex services that are connected by using a shared infrastructure, by integrating public services, cross-linking resources and allowing open access to base registries that facilitate collaboration while maintaining strict standards for data protection.
- The four interoperability layers - legal, organisational, semantic and technical interoperability.

[35] [LS14, p. 638] - Ana Lisboa and Delfina Soares 2014.
[36] [IDA16]
[37] [otEU10] - European Interoperability Framework (EIF) for European public services.
[38] [Com14] - European eGovernment Action Plan 2011-2015.
[39] [IP12]
[40] [Com17d]
[41] [Com16d]
[42] [otEU10]

The EIF further presents measures concerning its implementation in these sub-areas and addresses the formal definition of interoperability agreements as well as the requirements that governments will necessarily face when establishing the agreed-upon interoperability standards.

As the EIF plays a central role in regulating and establishing efficient and improved opportunities for police cooperation, its contents and significance will be discussed in greater detail in chapter 5.

CHAPTER 3

# Global, European and Austrian Police Cooperation

This chapter comprises an overview of the Europeanisation of police cooperation and provides the necessary political background that led to the evolution of the European Union (EU). It furthermore presents and discusses existing organisations that have been established to support and promote international and intranational police cooperation, focusing on the institutions' history and development in regard to technical, organisational and legal aspects of police data exchange.

## 3.1 Europeanisation of Police Cooperation

The establishment of institutions and organisations to prevent and control international crime on the European level is an ongoing collateral development during the political progression of the European Union itself.

This chapter addresses the history of European police collaboration, beginning with the establishment of the TREVI[1] Cooperation in the 1970s, moving from its first comprehensive reformation by means of the Single European Act (SEA) to being signed into action and the design of the Schengen Agreement. It introduces the foundation of the Three-Pillar-Concept of the European Union by the Treaty of Maastricht, the substantial changes concerning justice and domestic politics by the Treaty of Amsterdam, and their revision and expansion by the Treaty of Nice. Finally, it presents the Treaty of Lisbon, the attempt of the establishment of a European Constitution and the formation of the European Union in its present form, as well as the latest expansion of international data access privileges by the Prüm Agreement.

[1] [Kne01, p. 91] - "Terrorisme, Radicalisme, Extrémisme et Violence Internationale".

### 3.1.1 TREVI Cooperation

At the council meeting in Rome in 1975[2], the European Council initiated the installation of the TREVI group. At the group summit in June 1976 in Luxembourg the Ministers of Internal Affairs and Ministers of Justice of the member states - namely Belgium, West Germany, Denmark, France, Great Britain, Ireland, Italy, Luxembourg, and the Netherlands - defined the following fields of attention:

- Information exchange and data networks.
- Mutual support in combating terrorism.
- Exchange of technical knowledge.
- Improved communication between police officers.
- Cooperation in the areas of air traffic, nuclear power, and environmental catastrophes.

At first, meetings were held irregularly, but from 1986 onward the respective ministers met every six months. This and the signing of the SEA in that year set the course towards Europe-wide police cooperation.[3]

The original goal of TREVI was to ensure joint international efforts to counteract and prevent terroristic activity.[4] Over time the scope of TREVI activities was broadened to other areas of inter-European police work and many more tasks regarding internal affairs were integrated in the group's responsibility. Due to its relative secrecy and thus not publicly accessible modus operandi, a lot of criticism was aimed at TREVI, but the democratic deficits and covert character of the cooperation did not result in a decrease of its political popularity or executive competence. Since TREVI turned out to be the most effective tool of cooperation to date and provided convincing and significant results, member states overlooked its flaws and kept increasing the cooperation's area of responsibility.[5]

Up until the 1990s, the following specialised subgroups were formed within TREVI:[6]

- TREVI I addressed questions regarding terrorism and its control, immigration, and asylum politics. The group was entrusted with the provision of up-to-date situation reports and ensured extensive information exchange about terroristic activities. It was the origin of first strategies towards the establishment of central coordination structures, as for example the deployment and commission of liaison officers.[7]

[2] [Uni16d]
[3] [Käm01, p. 48-51] - Kämper 2001.
[4] [Kne01, p. 91]
[5] [Deg03, p. 22] - Degenhardt 2003.
[6] [Kne01, p. 92ff.]
[7] [Mut10, p. 29] - Mutschler 2010.

- TREVI II focused on general efforts to improved police cooperation, aiming at harmonisation of communication, forensics and data analysis within international and different intranational institutions. Their agenda includes the endeavours to support and promote education of executive organs (as for example through language courses), mutual exercises of special forces and agreements on handling and prevention of riots at major events.[8]

- TREVI III dealt with the prevention and control of international organised crime, including drug trafficking and drug-related crime.[9]

- TREVI-AG-Europol was tasked with the establishment of a European police office and a European headquarters for drugs and narcotics.[10]

- TREVI IV was installed to regulate and revise compensation measures for an eventual decrease in safety due to the removal of EU-internal border control.

The group of Home Secretaries of European Community (EC) member states responsible for TREVI were situated externally of the institutional framework of the EC. They were not eligible to make decisions on their own. Suggested agreements had to be ratified by the individual member states.[11]

### 3.1.2 The Single European Act

The Single European Act (SEA)[12] is the first reformation treaty of the Treaties of Rome that signed the European Economic Community (EEC) and European Atomic Energy Community (EURATOM) into action in 1957. It is the result and conclusion of a multi-annual reformation debate. By changing and extending the contracts of the EC it did not yet create a European Union, but it provided a foundation for the Treaties of Maastricht, Amsterdam, Nice and Lisbon.

The signing of the SEA took place after several important stages that followed the genesis of the idea of a European Union:[13]

- June 1983 – Declaration of Stuttgart, where heads of states and governments of the European Council made a ceremonial declaration for a European Union.[14]

- February 1984 – Draft for a Treaty for the foundation of the European Union.[15]

[8] [Mil03, p. 24] - Milke 2003.
[9] [Mut10, p. 29]
[10] [Sul99, Pape 20f.] - Sule 1999.
[11] [Mut10, p. 29]
[12] [Com87]
[13] [Uni16c]
[14] [Uni16e]
[15] [Uni16f]

- June 1984 – European Council of Fontainebleau, regarding compensation measures for the UK.[16]
- June 1985 – The European Commission submits a White Paper to the European Council regarding the opening of the European Internal Market.[17]
- June 1985 – The White Paper is approved at the Council of Milan, and first efforts towards the Schengen Agreement are initiated.[18]
- December 1985 – The Council of Luxembourg decides to change the Treaties of Rome and promotes the development of the SEA.[19]
- February 1986 – Signing of the SEA in Luxembourg and The Hague.[20]

As a contract under international law the SEA became operative on July 1st, 1987.[21] It combined two specific fields of topics:[22]

- The Agreement on European Political Cooperation (EPC).[23]
- The legal act changing the EC contracts in regard to the decision processes within the Council, the capacities of the European Commission and the European Parliament and the expanded authority of the EC.

Besides stating regulations and specifics regarding international collaboration, it also fortified the sovereignty of member states:

"Nothing in these provisions shall affect the right of the Member States to take such measures as they consider necessary for the purpose of controlling immigration from third countries, and to combat terrorism, crime, the traffic in drugs and illicit trading in works of art and antiques."[24]

### 3.1.3 Schengen Agreement

At the 1974 Summit of Paris the heads of states and governments of the EC had decided upon establishing the "Passunion" (German for "passport union"), an agreement that simplified border crossing between EC member states.[25] The idea of removing border

[16] [Uni16f]
[17] [Uni16g]
[18] ibid.
[19] ibid.
[20] [Uni16h]
[21] [Uni16i]
[22] [bUUoL19a]
[23] ibid.
[24] [Com87] - "General Declaration on Articles 13 to 19 of the Single European Act".
[25] [Kne01, p. 102]

controls only came into action during the efforts towards the signing of the SEA. The idea of a Europe without domestic borders was first initiated by France and Germany, who - with the Agreement of Saarbrücken - made the first step by removing border controls between their respective national territories. Belgium, Luxembourg and the Netherlands joined the agreement and opened their borders as well. With the European Commission presenting a White Paper regarding the opening of the Internal Market to the European Council in 1985, domestic borders between those five states were practically eliminated and the Schengen area was established.[26]

In 1990, the agreement was fortified and expanded into the so-called Schengen Implementation agreement (Schengen II). It come into action in 1993 and was extended across Greece, Spain and Portugal who joined the agreement - which was now called Schengen Agreement - during its implementation in 1995.[27]

The Schengen Agreement launched a new form of police cooperation and was essential and incentive for the acceleration of Europeanisation. Conferences in the presence of East European cooperation partners were held to improve international police cooperation when dealing with migration flow[28] and regulations regarding collaborations were drafted for a range of different tasks, such as:[29]

- Mutual legal and penal assistance.
- Trans-national observation.
- Trans-national immediate pursuit.
- Improvements of police telecommunication.
- Residence reporting requirements of foreigners.
- Information exchange regarding crime prevention.
- Communication between liaison officers.

By installing these regulations to unify, standardise and harmonise criminal prosecution as well as the commitment to mutual support and legal assistance, international police work registered increasing success, mainly in the area of crime prevention. A significant portion of these successes was the result of allowing international observation and hot pursuit.[30]

International observation constitutes the long-term secret observation of individuals who are observed for potential criminal activities in one of the Schengen countries when it is

[26] [Uni16g]
[27] [EL85]
[28] [Feh01, p. 44]
[29] ibid., p. 45f.
[30] [Obe98, p. 66f.] - Oberleitner 1998.

suspected that this person might also commit a crime in a different Schengen country. The term hot pursuit (or immediate pursuit) refers to criminals who have already committed a crime and are prosecuted in a Schengen country. With prosecution already in process, police executives are authorised to pursue criminals on national territory of other Schengen countries without their explicit consent, minimising bureaucratic obstacles. Still, the responsible authorities have to be informed if a hot pursuit is being executed.[31]

In April 1994, Austria joined the Schengen Agreement as "observatory member" and finally signed the agreement in 1995.[32] While it was already authorised to contribute to and participate in Schengen councils, it only achieved full membership in 1997.[33] The reason for this delay was the Copenhagen Criteria[34] that had been determined in 1993 in the Schengen Agreement, which required Austria to properly secure its borders to the Czech Republic, Slovakia, Hungary and Slovenia, since these were the external borders of the EU until the East expansion in 2004.

In addition, a Supplementary Information Request at the National Entry (SIRENE) office was established in Austria in 1997. The office acts as the bidirectional interface between the state and other Schengen countries, using the Schengen Information System (SIS[35] since 2013: SIS II[36]). SIRENE acts as an independent institution and is part of the Austrian Ministry of the Interior (Bundesministerium für Inneres, BMI).[37]

### 3.1.4 Treaty of Maastricht

The contract that formed the European Union (February 7$^{th}$, 1992) is called the Treaty of Maastricht. It constitutes two large reformations of the Treaties of Rome (1957) and the SEA (1986).[38]

Just as the White Paper for the finalisation of the European Internal Market in 1985 was presented to the European Council,[39] demanding to remove all domestic border controls for international traffic within what was later established as the Schengen area until 1992, a series of suggestions on how to compensate potential loss of safety was brought forward as well. Part of that was the promotion of intensified police cooperation in the fields of terrorism and drug trafficking,[40] which was included in the EU contracts side-by-side with the planned cooperation in the judicial and domestic politics fields.

A central change that was realised in the Treaty of Maastricht was the integration of the EC and other elements in the three pillars of a temple structure that served as a

[31] [Bre09, p. 46ff.] - Breitenmoser 2009.
[32] [Obe98, p. 58]
[33] ibid., p. 82f.
[34] [EL19b]
[35] [MC16a]
[36] [MC16b]
[37] [Obe98, p. 84]
[38] [WW07, p. 452] - Weidenfeld/Wessels 2007.
[39] [KV02, p. 14] - Kraus-Vonjahr 2002.
[40] [Mut10, p. 30]

concept for the legal sections of Europe's politics and responsibility areas. In this model, the EU itself represents a superordinate roof connecting the supranational EC (EEC, European Coal and Steel Community (ECSC), EURATOM) as the first pillar,[41] the clauses regulating the intergovernmental Common Foreign and Security Policy (CFSP) as second pillar[42] and the intergovernmental collaboration in the judicial and domestic fields as the third pillar[43].

The creation of the pillar model and its stipulation in the Treaty of Maastricht provided a legal framework for the existing cooperation efforts between the national states, stepping up to the necessity of new approaches due to the increasingly international character of arising problems that started to turn into issues of shared interest. The introduction of the CFSP and the first-time institutionalisation of the Europe-wide "Police and Judicial Cooperation in Criminal Matters" (PJCC) with the foundation of today's Europol (proclaimed as an official EU agency later with the Treaty of Lisbon) resulted in significant improvements of the previously practised bi- and multilateral cooperation, whose complexity and de-coordination hampered its success.[44]

The new form of cooperation, however, did not constitute a transfer of competence and authoritative capacity from the member states to the EU but instead got only raised to the level of intergovernmental cooperation. The legal enactment regulations of the EU itself, therefore, did not extend to these areas.

### 3.1.5 Treaty of Amsterdam

After the EU expansion to the south (Greece, Spain, Portugal) and the 1995 inclusion of Finland, Sweden and Austria had increased the number of EU member states to 15, further effort was made to reinforce the EU as an "Area of Freedom, Security and Justice" (AFSJ). With the Treaty of Amsterdam (1997) substantial changes regarding the judicial and domestic areas were put into action.[45]

To this effect, first and foremost regulations referring to the third pillar of the EU were affected by the reformation of the EU contracts, leading to a reduced version of the third pillar and legal fortification of the remaining elements.[46]

Clauses and terms regarding the PJCC were only expanded and modified, but an additional new legislative procedure was launched: Contrary to the international law contracts that previously had to be individually negotiated between the nations to adapt mutual legislation, it was now possible for the European Council to write law by unanimous decision by itself instead of having to involve the national parliaments or the European Parliament.

[41] [bUUoL19c]
[42] [bUUoL19e]
[43] [bUUoL19f]
[44] [Lit10, 57f.]
[45] [Mut10, p. 31]
[46] ibid.

The legal status and capacity of Europol were expanded as well, and the Schengen agreement was integrated with the EU contracts as a protocol, thereby anchoring the right of free movement of people between member states to the EU contracts as a stipulated privilege. Furthermore, all vested rights of the Schengen agreement, including all former decrees and the actual contracts, were transferred directly into the EU legislation, with the fields of immigration, asylum and visa politics as well as other areas concerning the free movement of people being integrated with the EC contracts.[47]

Additionally, the legal capacity of the ECJ was increased by expanding its responsibilities to the revision of the validity and interpretation of framework decisions, agreements, and their implementation measures, and the European Parliament was granted the right to be heard.

The stipulation of a designated apparatus for police cooperation, especially the commission of Europol, customs and other qualified authorities, as well as the closer cooperation between national judicial authorities and the harmonisation of penal provision between the member states indicated considerable progress in regard to police and judicial cooperation efforts.[48]

The Treaties of Maastricht and Amsterdam therefore provided a foundation for European integration and can be seen as a reflection of the member states' will to contribute to the evolution of the EC to a general political European Union.

### 3.1.6 Treaty of Nice

Even before the signing of the Treaty of Amsterdam, negotiations with 12 additional potential EU member states in Eastern Europe were conducted. The negotiations aimed at giving these countries the opportunity to join the EU in accordance with the Copenhagen Criteria that had been proposed in 1993 which has largely been integrated in the EU contracts with the Treaty of Amsterdam. Disputes between the existing 15 member states, however, had already given rise to a range of issues with the framework of the current form of the EU. Since these problems could not be solved on time, the Treaty of Amsterdam was in parts restricted to simply acknowledging problems instead of suggesting solutions.[49]

As a result of the ongoing debate surrounding a reformation of the EU that continued until after the new millennium had begun, the concept of a European Union as an Area of Freedom, Security and Justice which had originated from the Treaties of Maastricht and Amsterdam was revised again with the Treaty of Nice (2001). It mainly served to address the "questions left open in Amsterdam". One of its clauses, as an example, dismissed unanimous decisions as legislative procedure for many areas and replaced it with the acceptance of a qualified majority (supermajority) to decide legislative changes.[50]

[47] [Lit10, p. 61]
[48] ibid., p. 60
[49] [bUUoL19d]
[50] [Par19a]

The regulations concerning the PJCC eventually ended up being the only remaining element of the third pillar. However, provisions were made to further improve and interlink collaborations between police forces, customs, and other penal and judicial authorities.[51] The goal was to engage and oblige member states to cooperate, exchange information and facilitate communication.[52]

Nevertheless, the Treaty of Nice still was not meeting the objective of solving the Amsterdam issues and was harshly criticised by member states who saw their influence threatened. To amend the lack of satisfactory progress, a "Declaration on the future of the Union"[53] was included which already initiated further negotiations and prospective changes in the so-called Post-Nice process.[54] Main objectives were the Charter of fundamental rights of the European Union, which supposedly should have resulted in a common constitution for Europe.[55]

### 3.1.7 Treaty of Lisbon

The Treaty about the Constitution of Europe (2004) should have been put into action by 2006. It was intended to realise substantial changes within the EU[56] by unifying all existing EU contracts and replacing them with a single constitutional document. The ceremonial signing of the constitution treaty was already in process when negative results from referenda in France and the Netherlands brought the ratification and implementation of the treaty to a sudden halt. Despite the successfully executed EU expansion to the East in 2004 and 2007, the EU reformation efforts came to a standstill, eliciting an unprecedented crisis that lasted for two years. It was only overcome in 2007 when the German Presidency managed to convene the heads of states and governments in a new Intergovernmental Conference (IGC) and when the Treaty of Lisbon (2007) was drafted to finally secure the reformation.[57]

With the Treaty of Lisbon, the three pillars of the EU were ultimately brought together and the temple concept was abandoned. The AFSJ had to be newly organised and based on a fundamental standard, determined by various protocols and benefitting the instrumentalisation of framework laws to effectuate the now inherently and ubiquitously applied ordinary EU legislative procedure.[58]

The legal capacity of the ECJ was again and substantially increased and broadened. The last remaining element of the third pillar, the PJCC, was relieved from its exceptional position by splitting it into two individual fields of duty, namely the police cooperation

[51] [Mut10, p. 32f.]
[52] [Eur19b]
[53] [Eur01a]
[54] [Par01]
[55] [bUUoL19b]
[56] [Mut10, p. 33]
[57] [bUUoL19g]
[58] [otEU19b]

and the judicial cooperation in criminal matters and fusing them with the EC-contracts that have formerly been situated in the first pillar.[59]

The results and agreements achieved by the constitutional convention (which became operative in 2009) and particularly the communitarisation of the PJCC finally led to newly emerging advances towards a unified Europe and constitutes a vital contribution to the necessary progress within a union that faces challenges of international terrorism and organised crime.[60]

### 3.1.8 Prüm Decisions

In the wake of the political deadlock following the Treaty of Nice, Austria, Belgium, Germany, Spain, France, Luxembourg, and the Netherlands still agreed to sign the Prüm Decision (2005).[61]

The treaty is a derivation of a multilateral agreement which has so far been signed by 12 EU member states, Norway and Iceland, and serves as means to improve police and judicial cooperation in the areas of the prevention and control of terroristic activities and trans-national crime.

The Prüm decision comprises the following measures:[62]

- Measures to prevent terroristic offences (information exchange, commission of air traffic security personnel).
- Measures to combat illegal migration (assignment of document specialists, support for repatriation).
- Regulations concerning the consolidation of other trans-national forms of cooperation (mutual police operation, hot pursuit, support for catastrophes and grave casualties with trans-national consequences, reciprocal consultation).
- Data and information exchange for major events.
- Regulations regarding data protection and safety.

The Prüm Decisions provide a regulatory framework for the facilitation of information exchange. It allows police and judicial authorities unrestricted international and intranational access to specified databases of other authorities. These access privileges encompass DNA-analysis data, dactyloscopic data (fingerprints), and a variety of files from national vehicle registers. The contract significantly contributes to the sustainability of police work standards and helps overcoming the current safety challenges not only in the areas of terrorism and organised crime, but also in cybercrime.[63]

[59] [Die11]
[60] [Mut10, p. 34f.]
[61] [otEU05]
[62] ibid.
[63] ibid.

## 3.2 Police and Judicial Authorities

The establishment of international cooperation in police and judicial fields of action is essential for a world-wide combat against criminal activities. It relies on one hand on voluntary cooperation efforts made by the different authorities in the form of police organisations and consortia and on the other hand, as described in chapter 3.1, on stipulated agreements and regulations that are drafted and enacted within the framework of political unions.

On a global level, the largest and best-known police organisation is Interpol (International Criminal Police Organisation, ICPO),[64] while on European level this role is fulfilled by Europol (European Union Agency for Law Enforcement Cooperation).

The agenda of Interpol is to facilitate international police cooperation worldwide. The organisation started in 1923 as the International Criminal Police Commission (ICPC), changing its name to Interpol in 1956. Interpol is politically neutral and its work focuses in particular on questions regarding public security, crimes against humanity and the environment, organised crime, terroristic activities, drug trafficking, arms trade, white-collar crime and cybercrime.

Europol is the official Criminal Intelligence Agency of the EU. It has 28 member states. The organisation was founded in 1995 (as a consequence of the Treaty of Maastricht) and became fully operational in 1999. Europol focuses on improving the cooperation between the authorities of its member states and therefore distributes intelligence resources that aim at combating international crime.

Europol benefits from a policy that does allow fast information exchange on various routes, as opposed to Interpol, where written correspondence is the exclusive form of communication. Another advantage of Europol is of course provided by the relatively high homogeneity between the European member states regarding their governmental, judicial, and administrational systems compared to the global level.[65]

In 2001, Europol and Interpol joint forces in the form of a first cooperation agreement. This was followed by a whole range of initiatives and projects nurturing this connection, including aspects like data exchange and education of police officers as well as more specific areas like the control of counterfeit Euro bills. Collaborations and communication between Interpol and Europol are mediated via the liaison networks in Lyon and The Hague.[66]

In addition to police cooperation between organisations, judicial cooperation is coordinated by the EU agency Eurojust[67] as well as the European Court of Justice (ECJ)[68].

[64] [Int19g]
[65] [Lit10, p. 146]
[66] [Hol06, p. 82f.] - Holzer 2006.
[67] [Eur19b]
[68] [Eur16b]

In Austria, police cooperation mainly comprises the Austrian Federal Police and the Criminal Police Office.

### 3.2.1 Interpol

The International Criminal Police Organisation (ICPO), know under its short name Interpol,[69] is an internationally active police cooperation of 194 member states (eff. 2019).[70] Its headquarters are situated in Lyon, France, from where national police forces are coordinated. The organisation is the second-largest global entity after the United Nations (UN). Its formation is not the result of an international treaty, but depends solely on the principle of Voluntary Participation of its member states that are represented by official police authorities.[71]

The two main sources of revenue for Interpol are the statutory membership fees paid by the member states and voluntary funding of additional activities and special projects organised by Interpol. In 2018, statutory revenues provided 57 million Euros and voluntary contributions amounted to 80 million Euros, generating a total budget of 137 million Euros.[72]

Interpol is neutral. Its charter prohibits the investigation of political, military, religious or racist crimes, meaning that e.g. the prosecution of a person due to a violation of a national religious law will not be supported by Interpol's capacities.[73] Despite these standards, complaints and criticism during the last 10 years addressed problems with national authorities in non-democratic or democratic in name only states like China[74] and Turkey[75] who abuse Interpol's resources to prosecute and control oppositional politics, journalists and human rights activists, highlighting the necessity of reformations within the organisation.[76]

#### 3.2.1.1 History of Interpol

At the end of the 19$^{th}$ century, it became evident that the development of criminal structures across national borders had to be taken seriously as a new political challenge. Advancing industrialisation and the expansion of transport facilities opened up new oppertunities not only for the economy but also for criminal organisations. The first step towards the realisation of international collaborations was the foundation of the International Criminal Union (German: Internationale Kriminalistische Vereinigung, IKV) in 1889.[77] Soon thereafter, in 1895, European police specialists were invited to

[69] [Int19g]
[70] [Int19d]
[71] [Tri12, p. 1]
[72] [Int19k]
[73] [Int19i]
[74] [AE17]
[75] [Apu19]
[76] [Fou15]
[77] [RR96] - Rentzel-Rothe and Bellmann 1996.

Paris to be presented with a new recognition and identification system for criminals, the "Bertillonage"[78]. The system was then implemented over time in almost all European countries, but within decades it was replaced again by the dactyloscopic system (fingerprint method). This method proved to be effort-saving while being more reliable and was propagated worldwide by the 1920s.[79]

Although the IKV was destabilised during World War I, meetings like the 1914 Criminal Police Congress in Monaco and the 1922 International Police Conference in New York achieved first successes of international police cooperation. In 1923, new initiatives in this area resulted in the foundation of the International Criminal Police Commission (ICPC) at the International Criminal Police Congress in Vienna. The ICPC served as predecessor of today's Interpol and consisted of officials from several European countries, as well as China and Egypt. The United Kingdom (UK) followed suit in 1928, the United States of America (USA) only joined in 1938, although an US-American police officer had already participated in the first congress meeting.[80]

During World War II and the annexation of Austria into Nazi Germany, Hitler took command of the organisation, and useful ICPC documents and resources were misused to the benefit of the National Socialists' Regime. Consequently, when the process of European integration was initiated after World War II, a new foundation for cooperation between the western states for the purpose of reconstruction and peacekeeping had to be created. The original ICPC organisation was revived and in 1946 the UN granted consultative status to the organisation.[81] After having been a mostly European organisation in the beginning, the number of member states grew to 55 until 1955. In this year, a constitution for the ICPC was ratified and given its present-day name, the International Criminal Police Organisation (ICPO).[82]

In the 1970s, the European integration process and the consequential opening of the European frontiers sparked new discussions regarding police cooperation. In Europe, significant progress was achieved by the cooperation between trans-national organisations as there were for example the Pompidou-Group[83], the Viennese Club[84] and the Comité Européen de Lutte Anti-Drogue[85] (CELAD). Interpol, however, was heavily criticised during this time for its lack of participation in the combat against terrorism and for its cumbersome communication.[86]

By the 1980s, Interpol comprised 125 member states. After its headquarter's relocation

[78] [Pia16] - An anthropometric system developed by Alphonse Bertillon for the identification of people using body measurements. This was an early biometric identification method.

[79] ibid.

[80] [Int19f]

[81] [Lit10, p. 31]

[82] [Bri19b]

[83] Cooperation group on combating drug abuse and illicit drug trafficking.

[84] Ministerial cooperation group founded in 1978 as a result of the cooperation between Germany, Italy, Austria and Switzerland.

[85] Founded in 1989 by the European Committee in order to combat drugs.

[86] [Lit10, p. 30]

to Lyon in 1990, its infrastructure for information and data exchange with the national offices was greatly expanded. The improvement of the system resulted in the Interpol Global Communication System 24/7 (I-24/7).[87]

#### 3.2.1.2 Area of Responsibility

The goal of Interpol is to provide full support to all criminal police agencies and other entities that can help prevent or combat crime and which take national laws and human rights into account.[88]

As an organisation of different police authorities, Interpol does not command its own executive forces that are authorised to make arrests, but serves as an administrative network with the goal of facilitated communication and information exchange between its members.

Its responsibilities can be categorized into seven areas that were introduced and ratified by all member states at the 2017 General Assembly. The seven Global Policing Goals are:[89]

- Counter the threat of terrorism – by identifying and prosecuting suspects, increasing the cooperation of intelligence agencies and tracking financial transactions and arms trade.
- Promote border integrity worldwide – by establishing cooperation between border authorities and promoting global standards in the area of border control.
- Protect vulnerable communities – by identifying potential prevention measures, disrupting the profits of criminal trade and thereby protecting victims from exploitation and human rights abuse.
- Promote global integrity – by strengthening international jurisdiction standards and supporting investigative methods to combat white-collar crime and corruption.
- Curb illicit markets – by educating the public about the risks of illegal trade and developing new approaches for the identification and disruption of illegal markets and their financial sources.
- Support environmental security and sustainability – by increasing capacities for the prosecution of environmental crime, protecting biodiversity and environmental resources, and the elimination of potential profiting from environmental crime.

Interpol's global communication system, the I-24/7, is nonstop available for inquiries and provides all members of police authorities with permanent access to Interpol's 17

[87] [Int16]
[88] [Int19l]
[89] [Int19c]

databases. Not only personal information such as nominal and forensic data of criminal subjects is collected and made available. These databases comprise data on lost or stolen property, focusing on travel and other official documents as well. Furthermore, Interpol has extensive databases available that provide data on arms trade and organised crime networks, as well as one database that contains up-to-date information on for example missing people or fugitive persons or potential threats.[90]

In Austria, the Federal Criminal Police Office (Bundeskriminalamt, .BK) is in charge of the administration of the I-24/7 and allows all State Offices of Criminal Investigation (Landeskriminalamt, LKA) to access the system (eff. 2013: 23,310 inquiries[91]).

To maximise the use of existing services, Interpol regularly initiates diverse training and education programs. They address issues specifically associated with a certain region. The improvement of police capacities and abilities of police forces in South East Asia in the areas of terrorism (Project Sunbird) and migrant trafficking (Project Relay) are examples of this strategy.[92] In addition to Interpol's online-learning-platforms,[93] interactive workshops are annually held in all regions to provide members with standardised education and advanced training. Police officers are taught to properly and effectively work with the databases, and exercises that teach problem-solving skills, background knowledge and case studies are presented.[94]

### 3.2.2 Europol

The European Union Agency for Law Enforcement Cooperation (Europol) was established as part of the third pillar of the now obsolete temple model of the European Union, which constituted the Police and Judicial Cooperation in Criminal Matters (PJCC).[95] Europol's rationale is the combination and integration of bi- and multilateral agreements (TREVI, Schengen Agreement, European Drug Unit) in the form of intergovernmental cooperation.[96]

Today, Europol's legal basis is the Regulation (EU) 2016/794[97] of the European Parliament and the European Council that was signed on May 11$^{th}$, 2016, in which Europol's role as an official EU-agency was stated as follows: "Any operational action by Europol must be carried out in liaison and in agreement with the authorities of the Member State or States whose territory is concerned. The application of coercive measures shall be the exclusive responsibility of the competent national authorities."[98]

[90] [Int19j]
[91] [Rec17, p. 257] - Rechnungshofbericht zu Bundeskriminalamt 2015.
[92] [Int19b]
[93] [Int19e]
[94] [Int19h]
[95] [Zie96, p. 427]
[96] [Rat08, p. 29]
[97] [PotC16c] - Regulation (EU) 2016/794.
[98] [Uni12a] - Article 88 (3) TFEU.

Similar to Interpol, Europol is a legal entity with its own organs, but it is not an independent EU-wide organisation. Its executive has not had its autonomous investigative responsibility until 2002 and until today it is not authorised to self-reliantly make arrests. Instead, Europol collects information and distributes them to member states to increase the performance and capability of national authorities and improve their cooperation. Europol's first and foremost goal is to prevent and control serious international crime.[99]

Currently, Europol has 28 EU-member states and 1,294 employees, 243 of which act as liaison officers.[100] Its budget amounts to 122 million Euros (eff. 2018).[101]

Europol's responsibility lies in the areas of the combat against terrorism, the combat and prevention of international arms and drug trade, child pornography, money laundering, organised immigration crime and human trafficking.[102]

#### 3.2.2.1 History of Europol

First attempts of establishing a European Police Office were already made in the 1970s. After the fusion of ECSC, EURATOM and EEG to form the EC in 1967, the meeting of all EC heads of states and governments at the 1969 Summit of The Hague is considered the first step and milestone of European integration politics. Within the scope of the European Political Cooperation (EPC) that had risen from this meeting, the 1974 Summit of Paris resulted in the foundation of the European Council. The formation of a task force in order to examine the conditions necessary for granting citizens of member states of the EC specific rights (municipal election law, right of residence, "Passunion") was prompted.[103]

A major catalyst for the Europeanisation of police work was the criticism elicited by Interpol's communication and executive flaws, as well as the European Council's decision to promote enhanced cooperation in the areas of security and domestic politics. Based on the EPC and these developments, the TREVI group was founded in 1975, an served as a starting point of the European collaboration between police authorities in regard to domestic security. The group was originally intended to be a leading force in the combat against terrorism, but its responsibilities and activities soon spread across other penal areas as well.

Additionally to TREVI and its subgroups that got tasked with individual fields of responsibility to improve domestic security cooperation, the group for "Judicial Cooperation" (1975)[104] was founded. In the following years, a range of other groups followed, as for example the ad-hoc group "Migration" (1986),[105] the coordinators group "Freedom of

[99] [Zie96]
[100] [Eur19r]
[101] [otEU18b, C 108/143] - Official Journal of the European Union: "Statement of revenue and expenditure of the European Police Office for the financial year 2018 - (2018/C 108/28)".
[102] [Zie96, p. 427]
[103] [Hum96, p. 3f.]
[104] ibid., p. 7
[105] ibid., p. 9

Movement" (1988) that started to regulate the right of residence, the "CELAD"-group (Comité Européen de Lutte Anti-Drogue, 1989)[106] to combat drug trafficking and the group "Mutual Assistance" (GAM '92, 1992)[107] as a task force for customs administration.

Finally, in 1986, two years after the European Council had launched its designated program for a "Europe of Citizens", the Single European Act was signed, thus substantially reforming the EC-treaties and contractually stipulating the EPC for the first time. After the Fall of the Iron Curtain in 1989, the global changes in political systems and the consequential need for stable and peaceful solutions and agreements accelerated the European integration process. Up to this point, collaborations were only based on bi- or multilateral agreements mediated by the different task forces, but the suspension of EU-domestic borders led to a revival of the idea of a European Police Office. Therefore, another TREVI subgroup was founded in 1989, already being called TREVI-AG-Europol back then.

When the Treaty of Maastricht led to the foundation of a European Union as a Three-Pillar-Model, discussions about the Europe-wide police data exchange that had originated from a German initiative to install a central European drug unit, gained momentum. The member states of the Three-Pillar-EU decided unanimously that such an intergovernmental organisation has to be regulated by international law. Between 1994 (first draft by Germany) and 1995 the treaties concerning the new Europol Drug Unit (EDU) were negotiated and signed by the EU member states.[108] However, Great Britain refused to acknowledge the European Court of Justice (ECJ) as the last resort for the interpretation of the treaty. The country was granted an exclusion clause ("Opting-Out"), leading to a delay of the final ratification of the agreements until 1998. After a series of legal acts by several different authorities, Europol was finally able to take up its full function on July 1st, 1999. It replaced not only the EDU, but all former versions and groups that had been responsible for its establishment and realisation as well.[109]

The first cooperation between Europol and Interpol was agreed upon in 2001 in order to combat the distribution of counterfeit money.[110] In the same year, a cooperation with the USA regarding technical and strategical collaborations took place.[111] Following the fusion of the three pillars of the EU with the EC with the signing of the Treaty of Lisbon, Europol was given the status of a reformed and official agency of the EU and was integrated with the Union's legal entity in 2009.[112]

[106] [Hum96, 10f.]
[107] [Com90, No C 262/4] - Official Journal of the European Communities, C 262, October 17th 1990.
[108] [EL19a]
[109] [Eur99]
[110] [Eur01b]
[111] [Eur01c]
[112] [Cou09]

#### 3.2.2.2 Legal Status and Organisation

With the 1997 Treaty of Amsterdam it was decided that a substantial range of political cooperation within the concept of an Area of Freedom, Security and Justice (AFSJ), meaning that they should be subjected to the regulations stipulated in the EC-contracts – however, that excluded the PJCC which ultimately remained in the third pillar as its single element and received a special position: The European Council was able to unanimously realise decisions without consultation of the European Parliament and the European Commission.

Since Europol was not an agency of the EC, but an element of the third pillar its integration in the organisational structure of the EU was challenging and led to much discussion. Adversary commenters criticised that Europol was no individual organisation, but an instrument of intergovernmental cooperation between the member states, and closely intertwined with other institutions, mainly with the European Council.[113]

With the Treaty of Lisbon (2007) and the formation of today's structure of the EU, the three pillars were finally merged. The special position of the PJCC ended when it was seperated in two areas and subjected to the ordinary EU legislative procedure. The PJCC was split in the area of Judicial Cooperation in Criminal Matters and the area of Police Cooperation ,[114] Europol got installed as EU-agency. Its new legal foundation was stipulated by the European Council in 2009 and replaced the original Europol-Agreement from 1995. The agreement, therefore, changed Europol's status from an international organisation bound by international law to an agency that was funded by the overall budget of the EU.[115]

With the decision (EU) 2016/794 of the European Parliament and Council in 2016, the Europol-Agreement was reformed again. The new Europol-Agreement consisting of 77 Articles and two attachments (on categories of crime and personal data). It formally instructs the EU-agency Europol to take over the European Police Office and its responsibilities.

The extended tasks and innovations are the following:[116]

- Installation of mutual international investigative task forces.
- Representation of the European Commission and the member states in the Administrational Council of Europol.
- The executive director serving as legal representative and leader of Europol.
- The aggravation of data protection regulations concerning personal data, as for example stated in Article 18.

[113] [Lit10, p. 130]
[114] [Die11]
[115] [Cou09]
[116] [PotC16c]

- Europol is authorised to choose its own ICT structure to maximise efficiency and act as service provider.
- The obligation to cooperate with the European Data Protection Supervisor (EDPS).
- The role of the European Parliament in the supervision and investigation of Europol's activities.
- The employees of Europol are granted the statutes of EU-officials.

Europol is governed by a director, who is also the legal representative of Europol. He collaborates with three deputy directors who are the heads of the functionally separated departments[117] (Fig. 3.1).

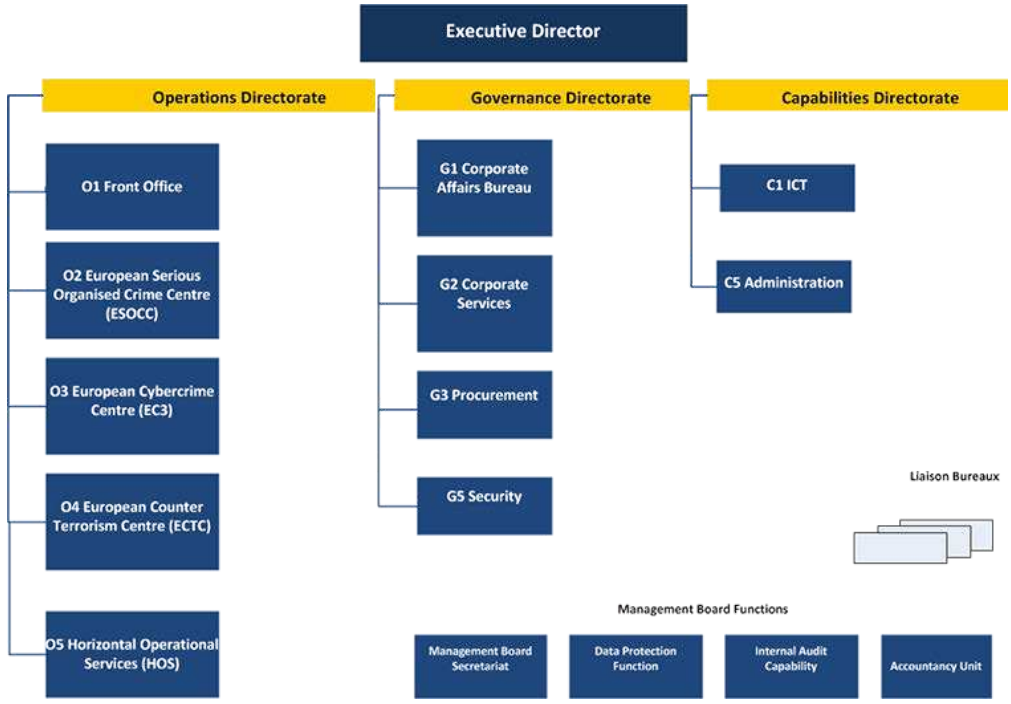


Figure 3.1: [Eur16c] - Europol's Organisational Structure (eff. 2017).

The Administrational Council constitutes a representative from the European Commission as well as a representative of each respective member state. They decide strategies and annual work programs of Europol, determine the budgetary plans and supervise the administration of the office of directors.[118]

[117] [Eur16c]
[118] ibid.

The 28 member states are associates of Europol. Operational contracts exist with "Albania, Australia, Bosnia and Herzegovina, Canada, Colombia, Denmark[119], Eurojust, former Yugoslav Republic of Macedonia, Frontex, Georgia[120], Iceland, Interpol, Liechtenstein, Moldova, Monaco, Montenegro, Norway, Serbia, Switzerland, Ukraine, United States."[121] Strategical contracts exist with "Brazil, China, CEPOL, ECB, ECDC, EMCDDA, ENISA, eu-LISA, OHIM, OLAF, Russia, Turkey, United Arab Emirates, UNODC, World Customs Organisation."[122]

#### 3.2.2.3 Operation and Responsibility

In each member states a specific national office serves as the interface between the respective member state and Europol. The relations between the Europol national office and other national authorities are dependent on the legislative in the respective country. In Austria, the national office is situated in department 2 of the Federal Criminal Police Office (Bundeskriminalamt, .BK): international police cooperation office 2.2, Europol national office and liaison office The Hague.[123]

The national office provides Europol with up-to-date information, responds to inquiries from Europol and raises requests with Europol reciprocally. It also contributes data for Europol's information storage collection.[124]

The contact between Europol member states is mediated by liaison officers who are subordinate to the national office and who represent the member states' stakeholders at Europol. They are responsible for establishing the communication routes between their states' national office and Europol and convey the exchange of personal data. Furthermore, the liaison officers participate in data analysis and are authorised to use Europol's databases for informational inquiries as well as for adding new information and thereby expanding the data collection.[125]

The liaison office for Austria in The Hague is responsible for the coordination of the exchange of information between the Ministry of the Interior (Bundesministerium für Inneres, BMI) and Finances and Eurojust and Europol, as well as for bilateral information which is exchanged via the Europol route. In total, 26 Austrian liaison officers work with Europol (eff. 2018), and "Second Experts" have been commissioned since 2000 for various organisational units over limited time.[126]

[119] [Eur17d, p. 13] - "Pursuant to Protocol No 22 annexed to the TEU and to the TFEU, the Kingdom of Denmark is no longer part of Europol as of 1st May 2017, as it has so far not exercised the option to fully participate in the Europol Regulation. In order to ensure cooperation between Europol and Denmark on key matters an Operational and Strategic Cooperation Agreement has been concluded."

[120] ibid. - "The operational agreements with Georgia and Ukraine and the strategic agreements with the United Arab Emirates, Brazil and China are signed, but not yet in force, pending ratification."

[121] ibid.

[122] ibid.

[123] [Bun19b]

[124] [fI18a]

[125] ibid.

[126] ibid.

In addition to the liaison officers, Europol employs 100 designated data analysis experts who compile comprehensive and regularly updated reports that serve as a measure of potential threats and as description of relevant groups and people operating within organised crime structures. They also issue situation reports and tendency reviews concerning terroristic activities in the EU as well as an annual Europol report.[127]

Europol's responsibility covers illegal drug problems, human trafficking, illegal migration, cybercrime, intellectual property crime, tobacco smuggling, counterfeit money, tax fraud, money laundering, tracking of property and asset value, organised crime and terrorism.[128]

Current developments show the emergence of a head-to-head-race between technological innovations in the combat of crime and the ability of criminal organisations and groups to adapt to this progress. The EU Serious and Organised Crime Threat Assessment report (SOCTA-report) from 2017 emphasises the necessity of counteracting. An example for such an adaptation of criminal activities is the use of drones that are deployed by smugglers, to traffic drugs while evading border control. Other Criminal developments are the exploitation of information shared in social networks for victim selection and strategic burglary. The SOCTA-report also addresses the importance of combating the progressive tactics of data encryption used by criminal groups.[129]

#### 3.2.2.4 International Position in Criminal Prosecution

The installation of a European Police Office proved not enough to successfully combat all forms of international organised crime, however, expanding the concept frame contributed to an improved level of cooperation between Europol and its partners (Interpol, USA, Canada, Switzerland, Russia, etc.) and third countries issuing cooperation treaties. Europol's international position has yet to be built up, as the current situation depicts problems and uncertainties regarding how partners classify Europol as an authority. Other countries and unions are still lacking the necessary level of trust in Europol. The result of this is that larger states such as the USA or Russia prefer bilateral cooperation with the respective European countries.[130]

Interpol acts from a monopoly position within the sector of international crime prevention and control. Being significantly older and as a result more experienced it is the global ringleader when it comes to fighting criminal activities such as terrorism, drug and arms trafficking or white-collar crime.[131]

Europol, on the other hand, leads the field of technology transfer and data exchange, its expertise with the most up-to-date ICT applications and methods being unmatched globally.[132] Europol's databases and communication systems grant the fastest and most

[127] [Eur16c]
[128] ibid.
[129] [Eur17d, p. 14]
[130] [Lit10, p. 144]
[131] ibid.
[132] ibid.

secure access of data and information, rendering its technical support and analysis capabilities the most effective amongst all other organisations and police authorities.[133] A noteworthy innovation for international police cooperation is the exchange of DNA-profiles, which has been contractually appointed within the Prüm agreement and heralds the start of a new era of data exchange.

#### 3.2.2.5 Exemplary Relevant Figures

In 2018, Europol employed 1,294 officials, 33% of which were female, who are categorised as 129 analysts, 292 experts/special force employees and 243 liaison officers,[134] and had a budget of 122 million Euros available.[135]

In order to meet the member states' requirements, Europol increased its capacities until 2016. It also established a European Migrant Smuggling Center as response to the increase in migration and refugee movements, as well as the European Terrorism Center and the Intellectual Property Crime Coordinated Coalition (IPC3).[136] The latter commands a database containing information on 22,000 suspects, with more than 50% of entries having been added in the year 2017 alone. This constitutes an enormous growth of this pool of information but it also mirrors the elevated rates of criminal activities.[137]

Moreover, 46,000 new cases in all areas of responsibility were initiated in 2016, amounting to an increase of 16% in comparison to 2015. The Europol annual report 2016-2017 presents impressive numbers: A staggering 870,000 operational messages were exchanged between prosecution authorities, Europol's databases were called upon to respond to 1.5 million search inquires by around 7,000 users residing in the 28 member states and approximately 10,000 experts of law enforcement were provided with network connections using Europol's platforms. All of this depicts a rapid increase in cooperation efforts between member states.[138] With the aid of the European Network of Fugitive Active Search Team (ENFAST), a special force for blitz operations aiming at localising and detaining fugitive criminals, Europol managed to coordinate the apprehension of 27 of the most wanted European criminals.[139] More than 5,000 international and mainly hierarchically structured organised crime groups residing in 180 nations are currently under observation. 76% of those consist of at least 6 members, 60% have their headquarters in EU member states, and around 70% are active in more than 3 countries.[140]

Europol's Deputy Executive Director, Luis de Eusebio Ramos emphasises the importance of electronic data processing systems and increased interoperability: "We will also continue to extend and improve Europol's core ICT systems in the wake of the Integrated Data

[133] [Lit10, p. 145]
[134] [Eur19r]
[135] [otEU18b, C 108/143]
[136] [Eur19m]
[137] [Eur17d, p. 7]
[138] ibid.
[139] ibid., p. 10
[140] ibid., p. 14

Management Concept (IDMC). The interconnection to European databases, especially (VIS) and possibly (EURODAC), will be complemented by the development of QUEST in parallel to the work of the Commission's High-Level Experts Group (HLEG) on Interoperability."[141]

### 3.2.3 Eurojust

To support and promote international cooperation between EU member states in the area of criminal prosecution and the judicial authorities' combat against transnational organised crime, the EU Unit for Judicial Cooperation (Eurojust) was founded. Eurojust specifically serves as platform for the exchange of information between national judicial and police authorities and coordinates trans-national criminal procedures on the European level.

Its area of responsibility does not only include the combat and prevention of terroristic activities, human trafficking, child pornography, and money laundering, but also the illegal trade of arms and drugs.[142]

#### 3.2.3.1 History of Eurojust

Eurojust was founded in February 2002[143] and resumed its work just months after. With the Treaty of Lisbon it was contractually installed as an independent EU agency.[144] Since 2003, its headquarters have been situated in The Hague. The rapid development from first drafts and the establishment of a provisional office called Pro-Eurojust in 2001 to a functional and fully active agency was fuelled amongst others by the terrorist attacks on the World Trade Center in New York on September 11$^{th}$, 2001, an incident that would change the world's view on terrorism and globally sparked efforts to push progress and enhancement of the combat against this form of organised crime.

The legal fundament for the installation of Eurojust was the decision of the European Council in Tampere 1999.[145] In the Treaty of Nice, which was intended to amend open questions from the Treaty of Amsterdam and reform the structure of the EU. Being a part of PJCC, Eurojust was placed within the third pillar of the temple model. In the course of the fusion of the three pillars of the EU, the Judicial Cooperation in Criminal Matters was split as an independent department from the PJCC and put under the control of the ordinary European legislative procedure. Eurojust was finally incorporated with the supranational EU law with the Treaty of Lisbon and regulated by interim arrangements during the five years following the commencement of the Treaty.[146]

[141] [Eur17d, p. 75]
[142] [Eur19d]
[143] [otEU02a]
[144] [Eur19b]
[145] ibid.
[146] [Cou08]

### 3.2.3.2 Structure and Organisation

Eurojust's member states each supply a representative to the Eurojust Committee or Council in The Hague. These representatives, who are recruited from the national pool of high-ranking judges or state attorneys - serve as a connective link between Eurojust and the national judicial apparatus and carry the responsibility for their respective liaison office.[147] The Committee elects a President and two Vice Presidents, the last election took place in 2016 (Vice President Klaus Mayer-Cabri from Germany) and 2017 (President Ladislav Hamran from Croatia and Vice President Filippo Spiezia from Italy).[148]

Eurojust is headed by an Administrative Director who reports to the Eurojust Committee's President and works hand in hand with a group of independent data protection commissaries who support the administration and supervise the agency's activities (Fig. 3.2).[149]

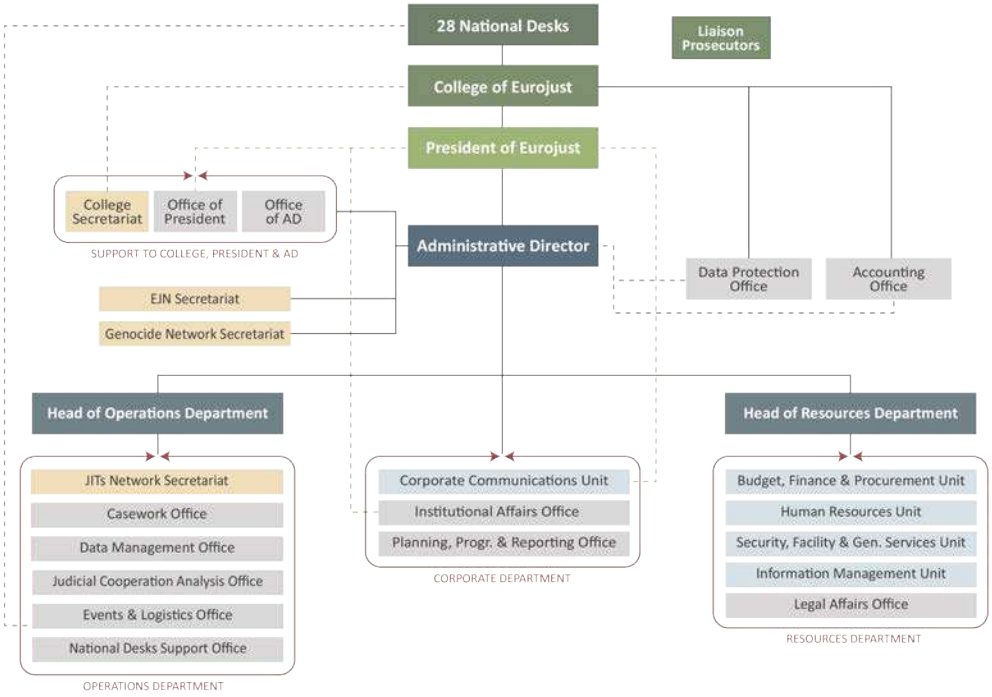


Figure 3.2: [Eur19e] - Eurojust Organigram (eff. 2018).

### 3.2.3.3 Areas of Responsibility and Legal Status

The expansion of the EU, especially the integration of a range of Eastern European countries (as for example former Soviet Union and Ex-Yugoslavia in 2004 and 2007) amplified the need for international cooperation which resulted in an active pursuit of

[147] [Eur17a]
[148] [Eur19a]
[149] [Eur19c]

prospects and regulations to exchange judicial information and personal data. Cooperation agreements were negotiated and unions created. Eurojust has a range of partners. Amongst others are:

- The European Judicial Network (EJN), founded in 1998 and incorporated into EU law as legal network in 2008.[150]
- Europol (see Chapter 3.2.2).
- The European Commission's Anti-Fraud-Office (OLAF), tasked with the investigation of potential abuse of the EU-budget, corruption and misdemeanour within European institutions.[151]
- The European Border and Coast Guard Agency (Frontex), handling border regulations and control within and around the Schengen area.[152]
- The European Union Intelligence and Situation Centre (EU INTCEN or SitCen), an intelligence agency of the European field service with important relevance in the area of trans-national cooperation between the EU and non-EU states.[153]
- The European Police College (Collège Européen de Police, CEPOL, see Chapter 2.1.3.3).[154]
- The European Judicial Training Network (EJTN), supporting the education and advanced training of judges and state attorneys.[155]

Right from the start Eurojust grew rapidly and its significance increased steadily. The existing set of regulations had to be revised and adapted continuously, a process that already transpired before its authorities were fully integrated with the EU-contracts with the Treaty of Lisbon.[156] To enhance Eurojust's operability and to harmonise its status with that of the member states Provisions were made. This led to efforts being focused on an improvement of its operative authority, a facilitation of information exchange and a closer collaboration between national authorities and Eurojust.

Additionally, a special legislative procedure that enabled the European Council to commission a European Prosecution Attorney (from the European Public Prosecutor's Office, EPPO) was installed. This is either based on a Eurojust decree with an unanimous decision of the European Parliament, or in response to a proposal of such a decree by at least 9 member states. The EPPO then takes up the prosecution of crimes that

[150] [Eur19f]
[151] [Com19b]
[152] [Age19]
[153] [EU 15]
[154] [Uni16b]
[155] [Net19]
[156] [Cou08]

are detrimental to the EU-budget.[157] The foundation of EPPO was already formerly suggested in the Treaty of Lisbon. Its installation was ratified by the EU and 20 member states in the Regulation (EU) Nr. 2017/1939.[158] It was intended to act as an independent EU-agency from its headquarters in Luxembourg. Its responsibilities include the control and prosecution of transnational tax fraud, abuse of EU funds, corruption, and money laundering. After the Netherlands and Malta joined in 2018, the EPPO now constitutes 22 member states. The agency is hoped to be fully operational and to process its first assignments starting in the end of 2020 or the beginning of 2021.[159]

In 2013, the legal framework of Eurojust was again discussed to be revised and adapted, and the suggestions were realised in 2018 when the Regulation (EU) 2018/1727[160] was ratified and implemented. The innovations were concluded by the agency itself as follows: "The Regulation establishes a new governance system, clarifies the relationship between Eurojust and the European Public Prosecutor's Office, prescribes a new data protection regime, adopts new rules for Eurojust's external relations and strengthens the role of the European and national Parliaments in the democratic oversight of Eurojust's activities."[161]

### 3.2.4 The European Court of Justice

The European Court of Justice (ECJ) is the highest judicial organ and last resort of the EU. Together with the General Court of the EU (EGC), it represents the judiciary power within the political system of the EU.

The ECJ is responsible for lawsuits filed by the European Commission (concerning violation of contract charges), for lawsuits filed by other EU authorities or by member states that are not directed at the Commission, as well as for preliminary ruling lawsuits. It is entrusted with the interpretation of EU and EURATOM law (Treaty on European Union Article 19, Treaty on the Functioning of the European Union Articles 251-281, ECJ charter). Completing the system, the EGC is the last resort for lawsuits filed by member states against the European Commission.

The ECJ comprises one highest-ranking judge of each respective member state. Court members are appointed for 6 years each, with 50% of the judges being exchanged every three years, ensuring a dynamic rotation. The General Attorney of the ECJ has a special role since, his function is to file a motion following the oral negotiations that serves as an independent and neutral suggestion for a verdict.[162]

[157] [Uni12a] - Art. 86 TFEU.
[158] [Cou17]
[159] [Com16b]
[160] [PotC18]
[161] [Eur19b]
[162] [Eur16b]

### 3.2.5 The Austrian Federal Police

In Austria, the term "police" describes the authorities, institutions, and executive of security administration, which itself is a collective term for law enforcement areas that are regulated by the Ministry of the Interior (Bundesministerium für Inneres, BMI) and its security authorities. According to their areas of responsibility, the police forces can be distinguished into the Safety Police and the Administrative Police. The former constitutes the executive forces who are responsible for the maintenance of public peace, law and order, whereas the latter covers specific matters concerning administrative law (for example finances, industrial law or municipal building inspectors).[163]

Originally, Austria commanded three essential law enforcement agencies, namely the "Kriminalbeamtenkorps" (detectives), the "Bundessicherheitswachkorps" which comprised the executive forces in larger cities, and the "Bundesgendarmerie" which was responsible for about two-thirds of the population on 98% of the national territory. They acted as civil forces but were armed and organised in a military like fashion. In 2005, the agencies were fused and now constitute the predominant Austrian law enforcement agency.[164] Together with the security authorities, the law enforcement agency forms today's Austrian Federal Police, employing more than 23,000 officials in about 100 police stations that are sized according to the population density of their area of responsibility.

The Austrian Federal Police is hierarchically organised and separated in three resorts. The states' district commissariats and the municipal police stations are the first authorities, followed by the respective states' police headquarters as second authority, and the BMI as third resort.

The BMI as top-ranking authority for security administration is split in five sectors. These are: The Presidial Sector (Administration), the General Headquarters for Public Safety, the Judicial Sector, the Service Sector and the Sector of Foreigners and Asylum.

#### 3.2.5.1 The Federal Criminal Police Office

The Federal Criminal Police Office (Bundeskriminalamt, .BK) is the central hub of Austria's criminal prosecution and acts as a focal point for international police cooperation. It originally was a part of the BMI. Following the German example in 2003, it was renamed and installed as an authority with restricted autonomy. This took place in accordance to the Federal Law on the Instalment and Organisation of a Federal Police Office (Bundeskriminalamt-Gesetz, BKA-G).[165] The .BK is under command of the General Director for Public Safety. It employs 700 officials in seven divisions which themselves consist of 26 offices and 53 departments (eff. 2016). The seven divisions are:[166]

[163] [TU 15]
[164] [Bun19a]
[165] [dB19a]
[166] [Bun19c]

- Division 1: Criminal Strategy and Central Administration.
- Division 2: International Police Cooperation and Manhunt.
- Division 3: Investigation, Organised and General Crime.
- Division 4: Criminal Analysis.
- Division 5: Criminal Police Support and Aid Services.
- Division 6: Forensics and Technology.
- Division 7: Corporate Crime.

The .BK acts as Interpol's central office, Europol's national office, as national SIRENE office of the SIS and as one of the 159 Financial Intelligence Units (FIU) of the Egmont Group.[167] All formal contacts between all Austrian and foreign security authorities have to be run by the .BK and are not to be processed directly by the subordinate police stations.[168]

Main responsibilities of the .BK cover the following areas:[169]

- Education and Research – The .BK is responsible for the education of Austria's police forces and offers advanced training as well as the initiation and organisation of international educational projects and programs. Research agendas focus on correct identification of new criminal phenomena and the development of respectively necessary instruments and measures that police stations are provided with.
- Crime Prevention – A special training concept of the .BK for currently more than 1,200 police officials aims at improving the forces' ability to cooperate with corporate and economic entities, non-governmental organisations and municipalities, and to initiate progressive campaigns concerning crime prevention.
- Criminal Analysis – As the foundation of police operations and investigating, the .BK supplies police management with professional operative and strategical analyses to enhance the quality of everyday police work.
- International Police Cooperation and Manhunt – As mentioned earlier, the .BK serves as information platform and contact for international collaborators. All services and communications with relevant foreign police and judicial authorities are processed here. Manhunt information is collected, and the national and international information exchange of the SIS is coordinated by the SIRENE office within the .BK. International cooperation is mediated by 26 liaison officers in 22 states and at Europol (eff. 2019).

[167] [Gro19]
[168] [Com16e]
[169] [Bun19c]

- Operative Investigations – The .BK initiates, leads, coordinates, and controls investigative processes concerning organised crime, violence offences and offences against sexual integrity, narcotics trade and crime as well as human smuggling and trafficking. Cold cases are reviewed as new observations, analyses and technologies emerge, multidisciplinary teams work on white-collar crime and other complex cases. This includes the combat against cybercrime and online fraud, counterfeit crime, illegal gambling and money laundering. The apprehension of criminally acquired property aims at disrupting criminal organisations sustainably. Additionally, the .BK supports and aids other organisational and investigative units by joining forces in the areas of witness and victim protection, criminal psychology and securing electronic evidence.

- Criminal Technology – A large part of crime scene evidence examination is performed at the .BK in the departments of Chemistry and Physics, Documents and Handwriting and the department of Biology and Microscopy. Individual-specific data like fingerprints and DNA are collected in a central police records register and compared with international databases.

- Finally, the .BK also serves as contact point for citizens. Therefore, specific registration offices for problems and issues in the areas of money laundering, drug analysis, cybercrime, child pornography, sex tourism, environmental crime, human trafficking and betting fraud have been installed.

CHAPTER 4

# Data Protection Law

Police cooperation is a process that relies on the ability of officials to exchange information and data of individuals and is therefore closely related to discussions about data protection. Privacy and data protection are stated as fundamental rights in the Universal Declaration of Human Rights of the United Nations (UN)[1], covering all kinds of personal data and their distribution. However, in regard to police work, this creates limits for data exchange and requires regulation of authorised access to sensible data.

This chapter gives an overview of the emergence and evolution of data protection laws and focuses on Europe as global pioneer. It deals with relevant data protection regulations concerning the EU, Europol, and the international police cooperation as well.

## 4.1 A Brief History of Data Protection

The issue of data protection is as old as the idea of collecting data about individuals. The process of a census is known to have already existed up to 4,000 years ago. It was not only used by the Babylonians, but also by the early high cultures in Egypt and Persia and in Roman Empire. There, the practise was extended, but discontinued after the Empire's downfall.[2] The Catholic Church might have installed some of the first data protection laws by binding priests with the Seal of the Confessional Secret, although this particular form of "data protection" proved to be prone to abuse. The modern idea of privacy developed between the 17$^{th}$ and 19$^{th}$ century when governmental record-keeping increasingly raised the question of what happens to the collected data.[3]

Data protection in the age of electronic information technology is faced with a whole range of challenges that increased drastically in complexity from their origins, when

[1] [Nat15]
[2] [Bri19a]
[3] [Sol16] - Solove 2016.

United States Lawyers Warren and Brandeis wrote down their definition of privacy as the "right to be left alone" in their publication "The Right to Privacy" in 1890.[4]

German occupation forces had used paperwork collected by local governments to clearly identify and deport individuals to concentration camps had given a painful example of personal data abuse.[5] After the second world war, the Marshall Plan was financed and implemented by the USA and Canada to aid the reconstruction of Europe.[6] To this effect, the Organisation for European Economic Cooperation (OEEC) was founded in 1948 to unify the struggling countries' efforts to re-build a peaceful and flourishing Europe.

Towards the late 1950s, the OEEC had outlived its purpose and fuelled by its success, got re-branded as the Organisation for Economic Cooperation and Development (OECD) to serve a more global function. The foundation of the European Coal and Steel Community (ECSC), the European Atomic Energy Community (EURATOM) and the European Economic Community (EEC) had set the course for a European Union. The USA and Canada signed the OECD Convention in 1960 and other countries followed suit, amounting to today's 36 member states which are from North America, South America, Europe and the Asia-Pacific, plus an additional 5 "key partner" countries (Brazil, China, India, Indonesia, South Africa).[7] The OECD covers 80% of the world trade and investment. It aims to solve international economic issues on a global level[8] and serves as a pioneer of data protection as well.

During the rapid increase of data collection and storage during the 1960s and 1970s, with hidden cameras and the emergence of computers and databases being criticised for their potential and increased capacity of unintended secondary use of personal data, data protection and the citizens' right of access to and control of their own personal data became an important social and political issue.[9] The establishment of the 1967 Freedom of Information Act (FOIA) in the US was the first to stipulate the right of individuals to access their personal data from state agencies[10], and the 1973 Swedish Personal Data Act as the world's first national data protection law[11] indicated the beginning of a new era of information exchange.

Consequentially, the OECD issued their first "Guidelines on the Protection of Privacy and Transborder Flows of Personal Data" (updated in 2013)[12] which are acknowledged globally as a fundamental set of privacy principles.[13] They attempt to harmonise national data exchange regulations, promote free information exchange, deconstruct international barriers and put focus on the prevention of differential developments in Europe and the

[4] [WB90]
[5] [Cha19]
[6] [Edi09]
[7] [OEC19c]
[8] [OEC19a]
[9] [Cha19]
[10] [Che19]
[11] [Pal02]
[12] [OEC13]
[13] [OEC19b]

USA. Shortly after, the European Data Protection Convention (Convention 108) was put into action in 1981.[14] To this date, 54 countries signed the Convention 108 (eff. 2019) which has become the backbone of international data protection and privacy legislation all over the world.[15]

In 1995, the European Council enacted another regulation, namely the Directive 1995/46/EC "Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data".[16] The Data Protection Regulation of Electronic Communication was addressed in 2002 with the Directive 2002/58/EC.[17] With the Treaty of Lisbon and the extensive changes to the EU - also in regard to police and judicial cooperation - the right of privacy and fundamental standards of data protection stated in the Charter of the EU were bindingly stipulated within the Treaty on the Functioning of the EU (TFEU)[18]. Ultimately, in 2015, the General Data Protection Regulation (GDPR) was installed as a supranational law of the EU, applicable in all member states since May 2018.[19]

Between 2015 and 2017, the number of countries that had national data laws increased by 10%, from 109 to 120[20]. While data protection laws are updated and promoted around the globe, Europe still was leading in 2012, when more than 50% of all national data protection laws were situated in European states.[21] Up to this day, Europe serves as a global pioneer in this field.

## 4.2 European Digital Single Market

The European Single Market[22] is a strategy to fully unlock the potential of the "four freedoms" of the EU. As stated in the Treaties of Rome, the ultimate goal of the Union is the "free movements of goods, persons, services and capital".[23] The Schengen Agreement and the Treaties of Maastricht and Amsterdam took first steps to decrease Europe's economical lag of the 1980s and catch up with the non-European developed world. Even after the Treaty of Lisbon certain issues, mainly in the service sector, have not been resolved, and the Union is still seeking improvement.[24] One effort towards a solid and dependable data protection legislation was the commission of a European Data Protection Supervisor (EDPS, since 2004). THE EDPS is an independent supervisory authority for European Institutions when it comes to adhering to data protection and privacy laws.[25]

[14] [oE19] - "Protection of Individuals with regard to Automatic Processing of Personal Data".
[15] ibid.
[16] [PotC95] - Directive 1995/46/EC.
[17] [PotC02] - Directive 2002/58/EC.
[18] [Mil19]
[19] [PotC16b] - General Data Protection Regulation - (EU) 2016/679.
[20] [Gre17, p. 1]
[21] [Gre12, p. 5]
[22] [Com16c]
[23] ibid. - Art. 26 (2) TFEU.
[24] [Par19c]
[25] [Eur03]

The data protection regulation contribute to the technical and ethical aspects of police cooperation and also have an imminent and important effect on the capability of Europol as well.

Because of the developments in the areas of electronic communication over the last decades, this idea was expanded to accommodate the free movement of data on the sector "Digital Economy" and adapted to fit the need of today's digitalised society. It resulted in the strategy for an EU Digital Single Market[26], which includes efforts to sustain the integrity of data protection. To the effect, the GDPR and Directive on Security of Network and Information Systems (NIS-directive) were put into action in 2018, and regulations concerning e-privacy[27] and electronic Identification, Authentification and Trust Services (eIDAS).[28]

### 4.2.1 Digital Economy

The term "Digital Economy" was mentioned first in the Japanese recession during the 1990s[29] and refers to any kind of business, economic, social or cultural process that relies on digital communication technology. It can be categorised in its three main components:[30]

- eBusiness (business in the form of computerised processes).
- eBusiness infrastructure (hardware/software, network technologies, telecommunication, human capital etc.).
- eCommerce (transfer of goods, e.g. online shopping).

The EU commission communicated in 2015 that only a small fraction of the potential of digitalisation is exploited in the EU yet and that the growth maximisation in the Digital Economy sector therefore is one of the essential building blocks of the EU Digital Single Market strategy:

"Within less than a decade, most economic activity will depend on digital ecosystems, integrating digital infrastructure, hardware, and software, applications and data. Digitisation of all sectors will be needed if the EU is to maintain its competitiveness, keep a strong industrial base and manage the transition to a smart industrial and services economy. 75% of the value added by the Digital Economy comes from traditional industries, rather than ICT producers, but the integration of digital technology by businesses is the weakest element. Only 1.7% of EU enterprises make full use of advanced digital technologies, while 41% do not use them at all. Digitisation also offers unprecedented opportunities to

[26] [Com15]
[27] [Par02]
[28] [Eur14a] - EU Regulation 910/2014.
[29] [Tap96]
[30] [Top18]

other economic sectors, such as transport (e.g. intelligent transport systems) or energy (e.g. smart grids, metering).".[31]

### 4.2.2 Strategy Objectives

The central aspects of the EU Digital Single Market strategy are free access to online products and services, the improvement of the conditions of digital networks and service and therefore promoting growth of the European digital and non-digital market.[32]

Several specific objectives are stated in the strategy communication, as for example:[33]

- Improved online access to benefit entrepreneurs by offering new opportunities for economic growth.
- Administrational efforts due to VAT[34] regulations should be reduced by applying new concepts of enterprise taxes. Furthermore, obstacles and limits that restrict trans-national online activities like differences in contractual and copyright laws, have to be eliminated by standardisation and modernisation.
- Parcel delivery has to be facilitated by increasing the capacities for international delivery, and country-based discrimination for international online shopping has to be prevented, thereby saving approximately 11.7 billion Euros, as the national delivery fees allegedly increase by 2- to 5-fold for international delivery.
- The process of geo-blocking that allows online sellers to deny certain member countries of the EU access or the ability to purchase goods and services from their websites and instead handle the purchase via third parties, which results in different prices has to be averted.
- An appropriate framework of conditions and requirements has to be established to create a beneficial investment climate for digital networks, innovative enterprises, and research.
- The development and promoting of cloud computing, big-data-tools and the "internet of things", as suggested by the "Freeflow of Data"-initiative to decrease the restrictions of the currently still fragmented market by setting standards for innovative services.
- Interoperability of new technologies has to be optimised and harmonised by norming interfaces and ICT systems as drivers for endeavours regarding the fifth generation of wireless communication, the digitalisation of manufacturing and construction processes (Industry 4.0), cloud services, mobile payment systems, cybersafety, eGovernment, eHealth, and eTraffic.

[31] [Com15] - Chapter 4. "Maximising the growth potential of the Digital Economy".
[32] ibid. - "Three pillars of the Digital Single Market Strategy".
[33] ibid.
[34] Value Added Tax (German: Mehrwertsteuer).

### 4.2.3 ePrivacy Regulation

A regulation that defines the correct handling and processing of electronic communication regarding cookies, tracking, Ad-blocker and similar functions will presumably be decided shortly and might be put into action by 2020 or 2021.[35]

The new regulation is said to prohibit the current use of cookies, under a penalty of up to 20 billion Euros. Electronic advertisements will only be allowed after explicit consent from the recipient, and users will be able to install Ad-blocker on their devices.

The key points suggested by the Commission will most likely encompass the following:[36]

- New electronic service providers like WhatsApp, Facebook and Skype will be obliged to adhere to the same standards of data protection and privacy as traditional communication providers.
- The safety level for individuals and enterprises will be equalised by applying stricter rules.
- New business opportunities that deal with the processing of content and metadata will be opened.
- Rules regarding cookies have to be simplified so that users can comprehensively understand what they accept or decline.
- To prohibit undesired communication via e-mail, SMS or automatic phone calls, Spam protection has to be modernised and adapted.

### 4.2.4 European Data Protection Supervisor

The European Data Protection Supervisor (EDPS) is an independent authority of the EU. It is entrusted with the constructive and anticipatory, responsible supervision of the adherence of other authorities and institutions to data protection and privacy regulations. According to Regulation (EU) 2018/1725, the post was established "with respect to the processing of personal data [...] for ensuring that the fundamental rights and freedoms of natural persons, and in particular their right to privacy, are respected by the Community institutions and bodies".[37]

The EU Commission is required to consult the EDPS "when adopting a legislative proposal relating to the protection of individuals' rights and freedoms with regard to the processing of personal data".[38]

[35] [ePr18]
[36] [Com17c]
[37] [Sup19, p. 77] - Regulation (EU) 2018/1725 - Art. 52 (2) - "European Data Protection Supervisor".
[38] [Sup18, p. 2] - "Opinion 4/2018 on the Proposals for two Regulations establishing a framework for interoperability between EU large-scale information systems.".

In a five-year-strategy from 2015, the current EDPS proposed ideas on how to supervise and counsel EU officials in regard to data protection consequences. It is stated that the adherence to data protection regulations is essential for the interoperability of IT-systems in the EU as Area of Freedom, Security and Justice.[39]

Important EDPS objectives for 2019 include:[40]

- Promoting a broader discussion about interoperability between IT systems.
- The expansion of supervision to cover Eurojust.
- Guidance for questions regarding technology and data protection (IT-governance and -management, Cloud-computing).
- Support for the Internet Privacy Engineering Network (IPEN).
- Stronger cooperation with the EU and international partners (European Data Protection Board (EDPB)).

## 4.3 General Data Protection Regulation

Since 1995, the Directive 1995/46/EC[41] had been the primary law in the regulation of personal data that can be retraced to identify an individual such as address, e-mail address, date of birth, telephone number, bank account number or identification.

By implementing the General Data Protection Regulation (GDPR), the EU set steps to harmonise national laws regarding data protection and privacy. The GDPR was decided upon by the European Parliament and came into force in 2016, and, after a two years' transition time, finally applies to all EU countries.[42] Notably, an EU regulation serves as a directly applicable legislation that is legally binding for all member states, as opposed to an EU directive which states specific results that the states are allowed to incorporate into and implement according to their national laws.[43]

### 4.3.1 Structure

The GDPR constitutes 11 chapters containing 99 articles and 171 clarifying comments, with the 11 chapters being:[44]

- General Provisions – describing the objective and scope of the regulation.

[39] [Sup18]
[40] [Sup19]
[41] [PotC95] - Directive 1995/46/EC.
[42] [PotC16b]
[43] [ttEU19]
[44] [PotC16b]

- Principles – the seven fundamental principles member states should adhere to in regard to data protection.
- Rights of the data subject – the data subject being an identifiable natural person.
- Controller and processor – stating correct handling of personal data - the controller as the legal person or authority determining the purpose of the data processing and the processor as the executive body that handles the data.
- Transfers of personal data to third countries or international organisations – defining the circumstances and correct procedure to transfer personal data and access authorisation.
- Independent supervisory authorities – determining how the adherence to data protection laws is safeguarded independently.
- Cooperation and consistency – regarding the regulation of the interaction between authorities entrusted with data protection.
- Remedies, liabilities and penalties – providing a framework on how to handle judicial issues including complaints, compensation and data subject representation.
- Provisions relating to specific processing situations – concerning, amongst others, situations like data processing in the context of employment, scientific and historical research purposes and existing religious data protection rules.
- Delegated acts and implementing acts – regulating the involvement of the Commission.
- Final Provisions – putting the GDPR in context with related legislation and adding administrative clauses.

### 4.3.2 Aims and Principles

Article 1 of the GDPR states the subject-matter and objective of the regulation:[45]

1. "This Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data."[46]
2. "This Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data."[47]

[45] [PotC16b] - Art. 1 (GDPR) - "Subject-matter and objectives".
[46] ibid. - Art. 1 (1) (GDPR).
[47] ibid. - Art. 1 (2) (GDPR).

3. "The free movement of personal data within the Union shall be neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data."[48]

The fundamental principles of the GDPR constitute:[49]

- Lawfulness, fairness, and transparency – where lawfulness is established by parameters as consent, the vital interest of the data subject, and the public interest.
- Purpose limitation – to restrict unnecessary secondary use and distribution.
- Data minimisation – to adequately decide the amount of personal data to be collected.
- Accuracy – to erase or rectify/update incorrect personal data.
- Storage limitation – to limit the usage of personal data for a longer time than necessary for the intended purpose.
- Integrity and Confidentiality – to appropriately secure personal data, and prevent unauthorised access and unlawful processing.
- Accountability – the controller is responsible for the adherence to the above principles.

### 4.3.3 Rights of the Data Subject

When personal data is collected, data subjects have to be informed about:[50]

- Scope of the data storage.
- Judicial basis of the data collection.
- Duration of the data storage.
- Data transfer to third parties.
- Data protection rights of the data subject.
- Right of revocation.
- Right of access.
- Current state of the procedure.

[48] [PotC16b] - Art. 1 (3) (GDPR).
[49] ibid. - Chapter II (GDPR) - "Principles".
[50] ibid. - Chapter III (GDPR) - "Rights of the data subject".

Additionally, data subjects have to be informed about their right to acquire a portable copy of their personal data in storage, their right to erase their data under specific circumstances and their right to litigate any automatic, algorithm-based decision. The data subject must be provided with contact details of the respective data protection supervisor in order to be able to issue complaints against data protection authorities.[51]

To verify the adherence to the GDPR Rights of the data subject, controllers are tasked with the establishment of appropriate measures to be incorporated in the development of business processes, products, and services. An example for one of these measures that meet the design requirements and standards of the GDPR article 25 (Data protection by design and default)[52] would be the pseudonymisation of a data subjects data to provide encryption.

Lastly, the consequences of the storage of personal data for the data subject have to be assessed upfront, according to GDPR article 35 (Data protection impact assessment)[53] and the processing activities have to be recorded in regard to purpose, category, and respites. These records have to be provided to the data protection supervisory authorities on demand, according to GDPR article 30 (Records of processing activities)[54]

Chapter III of the GDPR states - besides clarifications concerning the procedure and handling of personal data of a data subject - specific rights that can be invoked by the data subject:[55]

- Right of Access and Right of Portability – citizens are entitled to access their personal data and information to gain knowledge about how they are processed. On demand, a controller has to provide an overview of the collected data and a portable copy of the original data. The data subject has to be enabled to transfer personal data from one electronic data processing system to another without interference of the controller.

- Right of Rectification and Right to Object – citizens are entitled to have their personal data completed and updated by the controller without undue delay. The data subject can object to the use of their data for various reasons, as for example if the data are used for direct marketing purposes or scientific/historical/statistical research purposes on the grounds of the data subject's particular situation.

- Right of Erasure and Right to Restriction of Processing – the so-called "right to be forgotten" refers to citizens being entitled to demand erasure of their personal data within 30 days or restrict its processing under specific circumstances, as for example if the purpose of the collected data has been fulfilled, the consent to data

[51] [Com18c]
[52] [PotC16b] - Art. 25 (GDPR).
[53] ibid. - Art. 35 (GDPR).
[54] ibid. - Art. 30 (GDPR).
[55] ibid. - Chapter III (GDPR).

collection is withdrawn, or the personal data has been processed unlawfully. The controller is responsible for taking responsible steps to meet the demands. The right of erasure does not apply in cases where the processing of the personal data is necessary for the exercising of the right to freedom of expression and information, for scientific or historical research purposes, for the benefit of the public interest or for the exercise of official authority vested in the controller.

### 4.3.4 Liability and Penalties

The controller is obliged to promptly report data protection and privacy breaches to the data protection supervisory authorities. Reports have to be issued within 72 hours and affected data subjects are to be informed immediately if there is a chance of negative consequences. Processors are bound to inform the controller if they perceive any personal data protection breaches.

According to GDPR article 83 and 84, sanctions of such breaches are:

- Letter of reprimand for the first unintentional violation of the guidelines.
- Regular data protection audits.
- Administrative penalties of up to 10 million Euros or up to 2% of the total worldwide annual turnover[56] for violations of:
  - The obligations of the controller or processor according to articles 8[57], 11[58], 25-39[59], 42[60] and 43[61].
  - The obligations of the certification body according to the just mentioned article 42 and 43.
  - The obligation of the supervisory body according to article 41[62].
- Administrative penalties of up to 20 million Euros or up to 4% of the last total worldwide annual turnover[63] for violations of:

[56] [PotC16b] - Art. 83 (4) (GDPR) - "General conditions for imposing administrative fines".
[57] ibid. - Art. 8 (GDPR) - "Conditions applicable to child's consent in relation to information society services".
[58] ibid. - Art. 11 (GDPR) - "Processing which does not require identification".
[59] ibid. - Art. 25-39 (GDPR) - Breaches of the general obligations relating to the security of personal data, the data protection impact assessment and the general obligations of data protection officers.
[60] ibid. - Art. 42 (GDPR) - "Certification".
[61] ibid. - Art. 43 (GDPR) - "Certification bodies".
[62] ibid. - Art. 41 (GDPR) - "Monitoring of approved codes of conduct".
[63] ibid. - Art. 83 (5) (GDPR).

- The fundamental principles of data processing, including the regulations of the data subject's consent, according to articles 5[64], 6[65], 7[66] and 9[67].
- The rights of the data subject, according to articles 12-22[68].
- The regulations concerning the transfer of personal data to third parties or international organisations, according to articles 44-49[69].
- The obligations of member states, according to chapter IX[70].
- The instruction of the supervisory authorities or the temporary or permanent restriction of processing and transferring of personal data, according to article 58[71].

## 4.4 Data Protection Law and Europol

The General Data Protection Regulation (EU) 2016/679 (GDPR)[72] covers a broad range of applications, however it does not extend to the characteristic remits of police authorities and justice. Therefore, the advancement of data protection legislation included the harmonisation of minimal standards in the area of police and judicial work within the scope of a new directive (EU) 2016/680[73].

All EU member states have to enshrine the set minimal standards in their national legislation in accordance with this directive, designated the JHA-directive[74]. Together with the GDPR, directive (EU) 2016/680 serves as the general data protection framework of the EU.

In Austria, this precept has been met in June 2017, when the new national data protection law[75] was issued and put into action by May 2018, addressing and adapting Austrian data protection legislation according to the GDPR and directive (EU) 2016/680. The latter has been implemented in the third part of the new law, stating specific provisions for police and judicial areas, in particular regarding authorities' obligation to share information and concerned parties' rights in terms of disclosure, correction and deletion of information. The BDSG[76] is designated in paragraph 64 as the official regulation meeting

[64] [PotC16b] - Art. 5 (GDPR) - "Principles relating to processing of personal data".
[65] ibid. - Art. 6 (GDPR) - "Lawfulness of processing".
[66] ibid. - Art. 7 (GDPR) - "Conditions for consent".
[67] ibid. - Art. 9 (GDPR) - "Processing of special categories of personal data".
[68] ibid. - Art. 12-22 (GDPR) - Rights of the data subjects.
[69] ibid. - Art. 44-49 (GDPR) - Transfers of personal data to third countries or international organisations.
[70] ibid. - Chapter IX (GDPR) - "Provisions relating to specific processing situations".
[71] ibid. - Art. 58 - Investigative powers of the supervisory authority.
[72] [PotC16b] - General Data Protection Regulation (EU) 2016/679.
[73] [PotC16a] - Directive (EU) 2016/680.
[74] [otEU20] - Justice and Home Affairs.
[75] [dB20] - Bundesdatenschutzgesetz, BDSG.
[76] ibid. - "Österreichisches Bundesgesetz zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, BDSG, Bundesgesetzblatt I Nr. 165/1999, in der Fassung BGBL I Nr. 14/2019".

the requirements of the GDPR and directive (EU) 2016/680 for "the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data"[77].

The judicial fundament for Europol's personal data processing has been laid with the 1995 Directive 95/46/EC, which states that member states have to protect the privacy rights and freedoms of natural persons.[78]

For its work, Europol requires a large amount of sensible and personal data and has to be especially aware of and diligent in preventing violations of the rights of individuals. For this reason Europol's data protection efforts are supervised on several levels, which are:[79]

- A functionally independent Data Protection Officer (DPO) leads Europol's own data protection department and provides advice and guidance on established data processing methods and applications. The DPO also ensures the adherence to data protection regulations when personal data is processed and transferred between Europol and the member states.
- The EDPS, together with his assistant-supervisor and supported by IT-specialists, administrators and lawyers is responsible for the periodical review and inspection of Europol's adherence to data protection regulations. In collaboration with the DPO, the EDPS can visit Europol's offices and is entitled to access all files of Europol in terms of data processing. Inspections result in comprehensive reports that contain observations, opinions, and recommendations.
- Every member state is additionally supervised by a national supervisory authority who has access to and inspects data processing files of the national liaison office.
- A cooperation committee that constitutes of a representative of the national supervisory authority and a representative of the EDPS has an advisory function.

Still, critics refer to the work of Europol as a "collecting mania without control"[80], claiming that data protection supervisors are lacking competence for proper supervision.

In line with the recommendations of the EDPS, Europol seeks to improve and expand the interoperability of their data processing systems. One result of these efforts is the installation of the online platform Europol Dataprotection Experts Networks (EDEN) on which experts from the areas of criminal prosecution, representatives of private parties

[77] [PotC16a]
[78] [PotC95] - "Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data".
[79] [Eur19g]
[80] [Mon10] - "Sammelwut ohne Kontrolle".

and educational institutions exchange professional knowledge and reliable methods to promote data security.[81]

Practical problems with the harmonisation of data processing systems within the EU arose when the installation of new applications and databases in the former Eastern bloc countries had to be postponed due to a lack of modern electronic infrastructure and ICT-standards. A mutual and slight, but persistent mistrust between police authorities of the different countries may be the reason for the diverse levels on which systems are operated and data is processed. This effect is enhanced by language barriers that still hamper effective police cooperation. Although authorities promote English as the administrative language, language skills and acceptance are very heterogeneous across Europe and interpreters are needed, thereby increasing the financial effort necessary for police cooperation.[82]

[81] [Eur19g]
[82] [Lit10, p. 98]

CHAPTER 5

# Interoperability

As discussed in chapter 2, interoperability is "the ability to collaborate between different systems, techniques or organizations with the ability of independent, heterogeneous systems to work together seamlessly and exchange information efficiently, without the need for separate arrangements between the systems."[1]

In this chapter, an overview of the efforts to increase interoperability within the European Union in regard to information and data exchange is given by discussing the creation, implementation and contents of the European Interoperability Framework (EIF), as well as an excursion on how database networks are established.

## 5.1 European Interoperability Framework

> "Give an organisation a data exchange system, and you feed it for a day. Teach an organisation a framework, and you feed it for a lifetime." [2]

An interoperability framework (as opposed to the term interoperability as a property of system interfaces) is "an agreed approach to interoperability for organisations that wish to work together towards the joint delivery of public services. Within its scope of applicability, it specifies a set of common elements such as vocabulary, concepts, principles, policies, guidelines, recommendations, standards, specifications and practices."[3]. Therefore, such a framework comprises not only the IT-aspect, but also a consensus between participating operators in regard to application and handling of given technological opportunities.

National and regional interoperability frameworks aim at creating a uniform environment for the instalment of European public services. The Interoperability Solutions for

[1] [GKM+91] - IEEE Standard Computer Glossaries.
[2] Referring to: Confucius, *551 a. Chr. - †479 a. Chr. - Chinese philosopher.
[3] [otEU10, p. 2]

European Public Administrations (ISA) program should provide digital interoperability solutions for governments, businesses and citizens largely for free.[4]

After the first European Interoperability Framework (EIF) was drafted in the scope of the Interoperable Delivery of European eGovernment Services to public Administrations, Businesses and Citizens (IDABC) program in 2004,[5] interoperability as a central aspect of e-government was substantiated in the action plans 2011-2015[6] and 2016-2020[7] of the EU Commission's Digital Agenda for Europe[8].

The first action plan cited the European Interoperability Strategy (EIS) and the second version of the EIF with its 25 recommendations as "key documents" for the promotion of interoperability[9] and stated the goals of its implementation:[10]

- Collaboration of public administrations on the European level.
- Direct exchange of information between EU member states.
- Efficient and effective transnational public services and cooperation between authorities providing them.
- Collaboration between governmental administration and citizens.
- Collaboration between governmental administration and businesses.

The second e-government action plan (2016-2020)[11] was launched alongside other initiatives that were discussed and decided in the scope of the 2017 Digital Day in Rome, an event in honour of the 60$^{th}$ anniversary of the Treaties of Rome.[12] The update was a logical consequence of the innovations decided in the 2015 Strategy for the European Digital Single Market (see chapter 4.2), as the public service sector generates a fifth of the Union's GDP and constitutes almost a quarter of all professional EU-positions.

The new framework[13] offers public administrations clear guidelines for improving interoperability within its digital services while enabling faster access to more efficient and secure electronic infrastructure with less expenditure as well. At the same time, the quality of data will be increased and data analysis as well as processing will be facilitated in order to benefit decision making and legislation.

To this effect, the new EIF introduces the following essential functions or developments:[14]

[4] [Com16a]
[5] [otEU10]
[6] [Eur10]
[7] [Cou15] - Regulation (EU) 2015/2240.
[8] [Par19b]
[9] [Gø10]
[10] [otEU10, p. 5ff.]
[11] [Eur16a]
[12] [Com17b]
[13] [Com17d]
[14] [Eur16a] - Chapter 2: "Vision and underlying principles".

- Digital-by-Default: By designing applications and services by default in a way that facilitates access to and simplifies administrational procedures, citizens are encouraged to utilise digital public services as "tool of choice", thus saving authorities time and tax money.

- Once-only-Principle: Increased interoperability enables public administrations to exchange data, thereby eliminating the necessity of repeated data transmission between citizen and authorities.

- Inclusion and Accessibility: This refers to providing all citizens with equal access to public services and promotes digitalisation as a useful approach to prevent limitations in accessibility for disabled people, the elderly and disadvantaged groups.

- Openness and Transparency: Citizens gain access to their personal data and are provided with the necessary technical and administrational infrastructure to review and correct it if necessary. Users should have access to the progress and current state of their administrational affairs.

- Cross-Border-by-Default: Public administrations should be expected to provide their digital services on an international level and across borders.

- Interoperability-by-Default: Unimpeded exchange of data, information and the international character of digital services should be guaranteed within the EU. The National Interoperability Framework Observatory (NIFO)[15] is tasked with analysing and reviewing the National Interoperability Frameworks (NIFs) of member and associated states to promote assimilation with the EIF and consequentially the progression of the European Digital Single Market.

- Reliability and Security: Data protection, privacy, and ICT-safety should be guaranteed, and respective efforts should exceed the adherence to judicial frameworks and legislation. Cryptographic methods are to be employed to ensure proper regulation and verification of authorised access.[16]

The EIF serves as driving force and standardised fundament for existing and developing electronic public services across Europe. By advancing the agenda of the European Digital Single Market, Europe should become more independent of dominant international solutions. The comparably sophisticated and progressive European standards regarding security and safety in the ICT sector should be expedited as well. Member states are expected to supplement the EU measures with national efforts.[17]

[15] [Com16f]
[16] [Bü18]
[17] [IP12]

By 2016, the EIF's implementation program ISA had also been updated to ISA$^2$, this was led and coordinated by the European Commission.[18] The current revision timetable of 6 years will be held up to keep pace with the rapid developments in the ICT sector and the rise of new technological possibilities. An evaluation of the new EIF and its impact is planned for 2019.[19]

While the EIF had been expanded, specialised and advanced content-wise, its overall structure has remained more or less the same. The 47 updated recommendations are spread across the entire document and cover the three main aspects of the EIF.[20] These are the underlying principles of European public services that have to be acted upon, the conceptual model describing how public services are to be integrated to form complex services, and the discussion of the different layers of interoperability. The last point includes interoperability agreements that put the EIF's recommendations into effect and interoperability governance to regulate the adherence to these agreements.

Figure 5.1 provides a timeline of European efforts to increase interoperability.

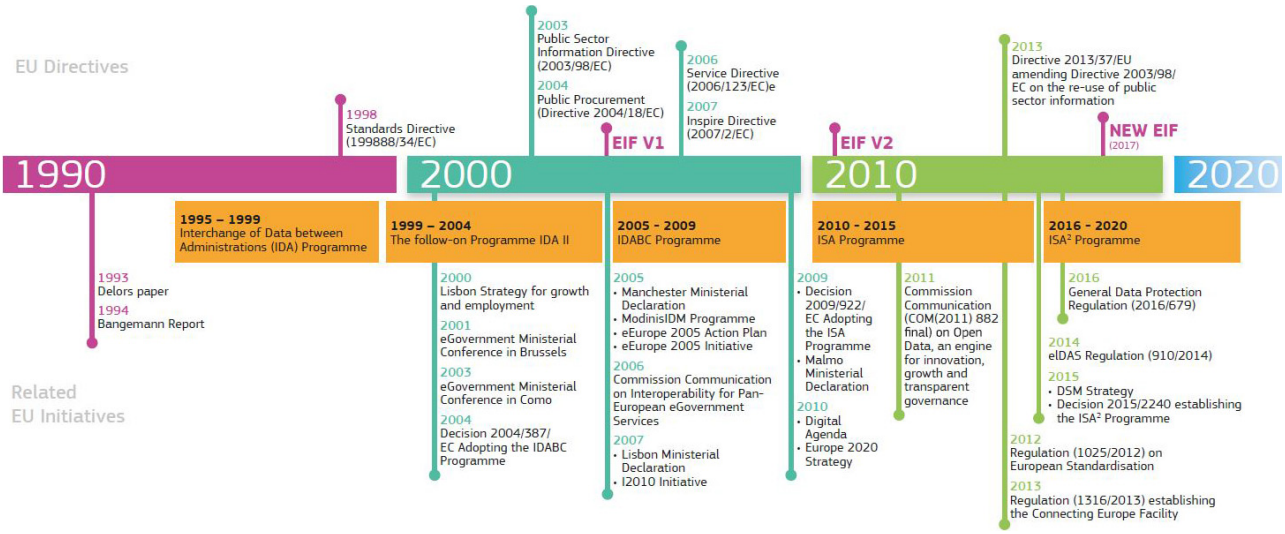


Figure 5.1: [Com16a] - "European Interoperability Timeline".

### 5.1.1 Underlying Principles of European Public Services

The new EIF constitutes a version of the original 12 principles that were adapted to today's technical and administrational possibilities, generating three categories:[21]

[18] [Com16a]
[19] Interview: DI. Dominik Klauser - ICT-Expert of the Bundesministerium für Digitalisierung und Wirtschaftsstandort (BMDW) and Austrian EIF Representative.
[20] [Com17d]
[21] [otEU10, p. 9ff.]

- The first principle is an individual category. It confirms the member states' subsidiarity as stated in the EU-contract, limits the right of intervention granted to the EU to an extent considered appropriate in regard to a given task, and thereby regulating collaboration on European level, internationally provided public services as well as the corresponding exchange of information.

- Principles 2-8 describe the general requirements (core principles) for international European collaboration. Furthermore, users' needs and expectations, they address user-centricity, accessibility, data protection, multilingualism and transparency.

- Principles 9-12 focus on concrete collaboration between national authorities and provide a fundament for unified standards for information handling, information exchange and for efficiency and effectiveness evaluation.

### 5.1.2 Conceptual Model for Integrated Public Service Provision

As stated in the focus points of the EU action plan 2016-2020, trans-European services should be designed for interoperability already in the planning stage. The reusability of services, information and data as an essential parameter of interoperability should be optimised as well.

The basic required elements for these efforts are visualised in Fig 5.2 and can be summarised as follows:[22]

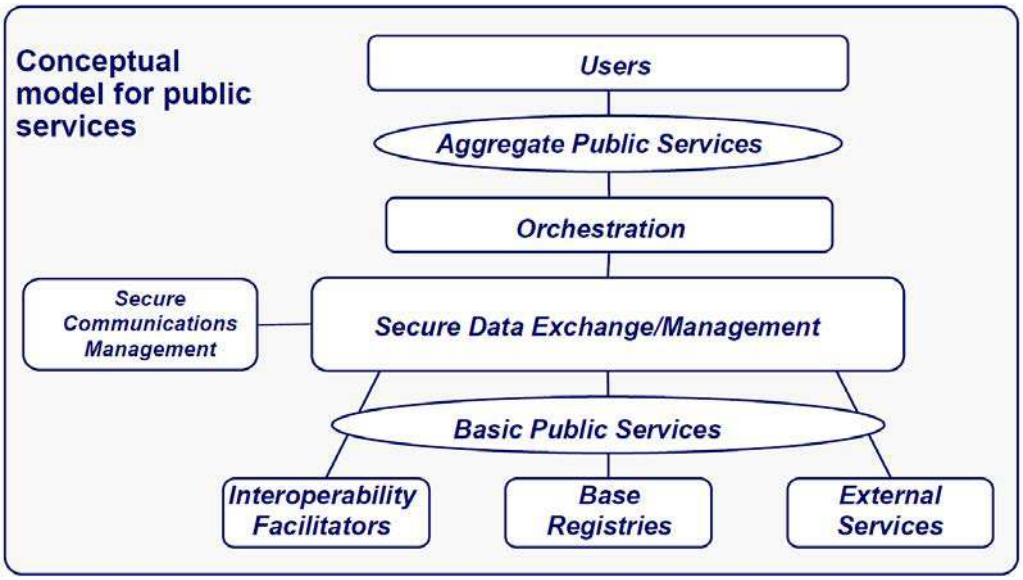


Figure 5.2: [otEU10, p. 14] - "Conceptual model for public services".

[22] [Com17d]

- Providing integrated public services – To enable international administration policies and to reduce the services' complexity for end-users, demand, development, execution, and evaluation should be orchestrated on the European level. This includes a "no wrong door policy" that allows access to public services via different channels while securing at least one digital channel (digital-by-default).
- Cross-linking internal resources and services – To prevent extra work due to misunderstandings caused by possible overlapping and discrepancies between information sources that are used by specific authorities, information and services should be made available for other institutions as well. The goal is a shared infrastructure that is expanded firstly by reusing information and services, secondly by allowing others access to new developments and finally by combining these interchangeable building blocks to create complex services. External resources provided by third parties are to be included.
- Establishing base registries, catalogues and open access – The basic and authorised information sources accessed by the governmental administration should be available and comprehensible for all users. At the same time, uniform methods to secure protection of sensitive data have to be developed. It is recommended to include metadata to describe contents and contexts of base registries as well as to use directories, glossaries and references to catalogue existing data and ensure easy access. New developments and implementations, as well as corresponding metadata, should be published in high quality and be referenced, machine-readable and non-proprietary.
- Data security and data protection – On a technical level, digital services should be developed using a "privacy-by-design" and a "security-by-design" approach to ensure data security as the highest imperative of all public services. On an administrational level, this is addressed by consistent, up-to-date risk management, efficient back-up- and recovery plans and clearly stated rules and precise monitoring of authorised access.

The model for public services fundamentally relies on base registries, external sources and interoperability solutions, governed by public administrations and subjected to appropriate data protection and security precautions.

Base registries serve as reliable, operative sources for basic information (persons, businesses, vehicles, buildings, locations, permits...), while external sources can include payment services offered by financial institutions or infrastructural services by telecommunication providers. Interoperability solutions are provided by information brokers that help for example with the translation between formats, languages, and protocols.

Additionally, data protection and security occupy a central and essential position of the concept, as any kind of access to basic digital public services requires electronic data exchange. To ensure data protection and security, all data has to be signed, certified and encrypted, and each data transfer or processing of data has to be logged.

Secure data exchange, therefore, requires different administrational tasks:[23]

- Administration of the public service itself, i.e. supervision of the entire communication between services, including the surveillance of access authorisation and audits.
- Registration of public services to grant access authorisation only if purpose, reliability and location of the access request are identified and verified.
- Comprehensive logging and cataloguing of all service activities, to allow post-processing monitoring, error information retrieval and to uphold quality standards.

Taken together, these efforts to integrate public services on local, regional, national and European level would allow for complex public services to be perceived as unified and intuitive by users (administrations, businesses, citizens) while assuring proper handling of sensitive data and security for their "digital persona". However, adopting the conceptual model might be obstructed by the utilisation of obsolete systems and their respective data repositories. Adaption is often complex and pricey. These limitations further emphasise the need for a semantic and technical standardisation of interfaces in order to enable transnational information exchange.[24]

### 5.1.3 Interoperability Layers

The development of a new European public service as a direct consequence of new EU-wide legal regulation has to state its area of application, priorities and necessary resources for the establishment and operation of the service right when the regulations are adopted. To improve international operability, political support and assistance are necessary. The new EIF, therefore, recommends that governments assign a high priority to the concept of interoperability as an essential tool for efficient international and intranational collaboration and provide the consequentially needed resources for its realisation. As a multi-dimensional issue, interoperability can only be optimised if awareness of its necessity is promoted and it requires competent handling and administration in four layers: legal, organisational, semantic and technical interoperability. Additionally, interoperability governance describes the regulation and supervision of the suggested interoperability measures and influences all four layers.[25]

#### 5.1.3.1 Legal Interoperability

Since EU member states act within the boundaries of their legislation, legal interoperability ensures the necessary framework for the collaboration between organisations that are bound by different political concepts and judicial strategies.

[23] [otEU10, p. 16]
[24] [otEU10] - EIF Recommendations.
[25] [Com17d]

The first step to take is to perform an interoperability check to identify existing national legislation that constitute a potential hindrance for new interoperability implementations. This might apply to restrictions regarding the usage and storage of data, strict regulations regarding the required quality of digital technologies provided by public services, differential data license models, contradictory requirements concerning otherwise comparable business processes and outdated data protection regulations. These issues and their impact on interoperability should be addressed before new services or implementations are installed and reviewed periodically for existing instalments.

To minimise conflicting legislation between member states, the ICT sector and respective implementations have to be discussed and considered already on the level of judicial procedure, with the digitalisation of European public services as a prioritised objective. Examining legal propositions regarding their digital realisation can thusly[26]

- ensure the eligibility and feasibility of new laws for not only physical but also digital environments,
- identify potential obstacles for digital data exchange and
- identify and asses ICT-related consequences for stakeholders.

Furthermore, clearly stated rules have to define in specific cases the handling of differential conformities to the law . If regulations in different EU member states are mutually incompatible and render a collaboration difficult or impossible, a jurisdictional decision has to be made to solve the problem and to maintain a legal force of information exchanged between member states.

#### 5.1.3.2 Organisational Interoperability

To establish European public services, a variety of administrational authorities has to collaborate efficiently and effectively, therefore organisational interoperability mainly aims at unifying procedures, responsibilities, business processes and expectations regarding common goals with mutual benefit. This includes the documentation, integration and harmonisation of business processes and exchanged information. The user community needs to be provided with easily available, accessible and user-oriented services.[27]

Besides aligning business processes, relations between service providers and users have to be defined properly and in detail. In order to do so, tools for the establishment of formalised standards that regulate the mutual support between public administrations and coherent handling of user demands must be defined. The Service Level Agreement (SLA)[28] and the Memorandum of Understanding (MoU)[29] are such approaches.

[26] [Com17d, p. 27]
[27] ibid., p. 28
[28] [otEU10, p. 34]
[29] ibid., p. 32

In any case, it is necessary to either align existing business processes or alternatively establish new ones.[30]

#### 5.1.3.3 Semantic Interoperability

Semantic interoperability ensures the comprehensibility of exchanged data and prevents its loss during transfer between users. Formats and meanings of data have to be preserved in their original form across all exchange procedures and all parties handling and processing the exchanged information must understand the defining parameters.[31]

In the scope of the EIF, the semantic aspect refers to the vocabulary and schemata of data elements and the relations between them. The syntactic aspect concerns the exact description of data format and grammar of the information to be exchanged to prevent the introduction of interpretational errors. This requires precise definitions, extensive documentation and information management strategies of a highly sophisticated level to avoid fragmentations and excess work. It is of importance to also manage and prioritise meta-, master-, and reference data as well, to ensure semantic integrity of exchanged data and information.

In Europe, the highly divergent national characteristics regarding language, culture, legislation and administration present a substantial challenge that opposes the efforts to standardise semantic interoperability. The lack of a certain degree of maturity of the collaborating nations impedes the seamless exchange of information, free data exchange and provision of data portability. This problem must be sorted out so that a functioning European Single Market can be created. Therefore, initiatives that aim at increasing semantic interoperability focus on cross-sector collaborations with national projects to establish fundamental principles and standards regarding this layer that European public services should conform to. Support in this area comes from advisory services supervising the drafting and implementation phase as well as web platforms that offer semantic interoperability solutions.[32]

#### 5.1.3.4 Technical Interoperability

On a technical level, the interoperability of systems used and standards that are necessary for data exchange has to be optimised. Technical aspects of information system coupling are interface specification, data presentation and exchange and network and data integration services. Formal specifications that are published by forums and consortia in the IT-sector have to be used.

Due to the sheer size of public administration and the fragmentation of ICT strategies, outdated systems are a major obstacle in this layer. Traditionally, these systems are developed following a “bottom-up” concept that fits the new solution to a specific problem.

[30] [Com17d, p. 28]
[31] ibid., p. 29
[32] ibid., p. 30

The lack of farsightedness in older systems leads to fragmented ICT islands that are hardly able to interact with others and require updating.[33]

It is therefore essential to develop open specifications that can be applied to all kinds of interfaces and ensure that new instalments and public services can be integrated into the network and that technical interoperability is promoted by default.

#### 5.1.3.5 Interoperability Governance

Besides the four layers of interoperability discussed in this chapter, interoperability governance constitutes a final component that spans all four layers. It serves as a "background" layer to the others and refers to how European public services are monitored and maintained with respect to their various interoperability aspects. This includes national and EU-wide decisions concerning existing interoperability frameworks, institutional regulations, administrational structures, strategies, agreements, responsibilities, and areas of action.

The Main focus points are:[34]

- The EIF itself, including updates and expansions.
- The action plans for interoperability which will be renewed in 2020.
- The European Interoperability Reference Architecture (EIRA)[35], a content model released by the European Commission that provides terminology and standardisation of ICT-solution building blocks that can be reused and aids public administrations with the implementation of new public services.[36]
- The INSPIRE directive, providing guidelines and an infrastructure to improve legal interoperability, coordination structures and technical requirements.[37]

Interoperability Governance is key to a wholesome concept of interoperability and transnational cooperation in all sectors and communication, coordination and management of all layers which has to be promoted. Therefore, support by the government is essential to enable public administrations on various administrational levels to collaborate and increase interoperability across sectors and national borders. The EIF clearly states the necessity of prioritising these efforts with appropriate intellectual and physical resources.

[33] [Com17d, p. 30]
[34] [Eur17b] - European Interoperability Framework – Implementation Strategy.
[35] [Cou15] - European Interoperability Reference Architecture (EIRA) - Decision (EU) 2015/2240 on ISA$^2$, Art. 3 (f).
[36] [Int19a]
[37] [Com19a]

To this effect, the ISA[2] program and the National Interoperability Framework Observatory (NIFO) specifically state the following aspects as tasks that have to be taken on and solved through proper interoperability governance:[38]

- Identification of normalised standards that cover a broad range of specific requirements and applications (according to EIRA).
- Assessment and evaluation of these standards and specifications with transparent, fair and likewise standardised methods.
- Implementation of these standards according to action plans and practical purposes.
- Surveillance and monitoring of the national and Europe-wide public administrations' adherence to these standards and specifications.
- Coping with the fast-changing challenges and new developments in the ICT sector by applying appropriate and up-to-date procedures.
- Documentation of standards and specification within itself standardised terminology, semantics and syntax in open databases and catalogues, foremostly the European Interoperability Cartography (EIC).

## 5.2 Database Cross-linking

In current developments, negotiators from the EU Parliament and the ministers' cabinet agreed to employ new functions to information systems containing biometric data in February 2019.[39] In April 2019, two separate decisions were published and it was decided "to interconnect a series of border-control, migration, and law enforcement systems into a gigantic, biometrics-tracking, searchable database of EU and non-EU citizens".[40]

This will result in a biometric data storage system filled with hundreds of millions of fingerprints and facial recognition data that are referenced with personal data. Its installation will be realised at the European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA) in Tallinn. The agency will also be responsible for the security of data transmission and technical administration of the system.

The directives regarding the interoperability of EU information systems in the areas of police and judicial cooperation, asylum, migration, borders and VISA have yet to be revised, published and legally signed into action by a formally adopted decision of the EU Council and Parliament before the effective technical implementation, which is planned for 2020-2023.

[38] [Eur17b] - European Interoperability Framework – Implementation Strategy: Action plan for interoperability.
[39] [Mon19]
[40] [Cim19]

The new laws will predominantly have consequences for the largest European manhunt and search database, the Schengen Information System (SIS II), which will be interconnected with the fingerprint database European Asylum Dactyloscopy Database (EURODAC)[41] and the Visa Information System (VIS)[42]. To establish a proper interoperability interface between the databases, the German Federal Police Office has introduced a new obligatory Universal Message Format (UMF)[43] for all member states. Additionally, a new search engine called Querying Europol Systems (QUEST) will be developed to enable inquiries to all three databases and also establish a link to data from Europol and Interpol each time a person is vetted.[44]

In the process of such an inquiry, biometric data will be fed into the Common Identity Repository (CIR). It enables inspectors to either add a new entry to the system or cross-check with existing fingerprints via EURODAC data, facial images via a Biometric Matching Service and finally the Schengen information regarding the identification of the vetted individual. By combining all this information, a Multiple Identity Detector that runs in the background can identify biometric data that has been linked to more than one matching identification or travel document, mainly using EURODAC's search system attributing fingerprints to several identities. If a query yields a match, an Identity Confirmation File is created for the associated individuum, prompting authorities encountering the respective individual to double-check and, if necessary, correct their biometric and identification data. A technical obstacle here is the development of an algorithm that indeed corrects for small spelling mistakes in the data but still does not raise adversarial errors in different nations.

Besides the existing three databases, an additional three new and central systems will be implemented and cross-linked for interoperability:[45]

- The Entry/Exit-System EES which stores biometrical data of all third-country-nationals (non-EU citizens or individuals from states that are not part of the European Economic Area, including Switzerland) upon crossing EU external borders.
- The European Criminal Records Information System for Third-country Nationals (ECRIS-TCN) that constitutes a database of criminal convictions of third-country-nationals residing within the EU.
- The European Travel Information and Authorisation System (ETIAS), which requires travellers to register their time, purpose, and planned itinerary for any period of residence in the EU, even without a visa. ETIAS will also have access to the Europol Information System (EIS) and it is estimated that this specific

[41] [Com18a]
[42] [MA16]
[43] See chapter 6.1.2.
[44] [Mon19]
[45] ibid.

cross-link will raise data traffic within this system enormously, increasing from 100,000 inquiries per month to potentially the same number of inquiries per day.

All other existing databases will remain present in their current form, but the project interoperability will also combine them in a mutual "data pot", as depicted in Fig 5.3. A central storage system for reports and statistics will be installed to record and trace all data storages and queries.

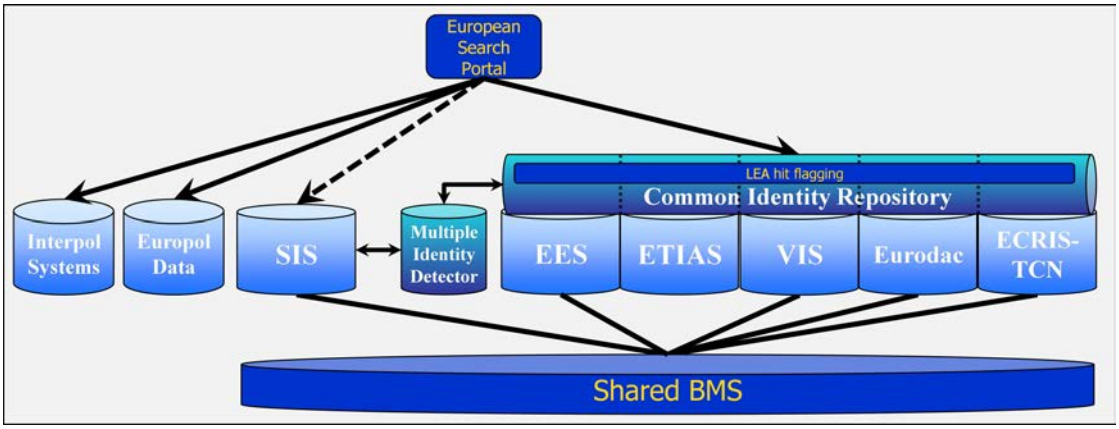


Figure 5.3: [Eur17c] - "European Search Portal (ESP) and the different databases and their partial interconnection".

In 2023, the implementation of the database cross-linking should be finalised and the new functions evaluated. After that, the border control organisation FRONTEX will be responsible for the surveillance of all interconnections made within the CIR and serve as the infrastructure for the central unit of ETIAS.

The EU Commission estimates the cost of realising the project interoperability to reside at 425 million Euro. In addition, the costs for EES are estimated to be 480 million Euros, the costs for ETIAS to be 215 million Euros and the costs for the updated version of the SIS II to be 68 million Euros. The development of EURODAC and VIS have not been subjected to cost estimations yet. The funding for these innovations will be provided by the European overall budget, the linking procedures and necessary infrastructural alterations have to be paid by member states and Europol, respectively.[46]

The CIR is going to be an incredulously massive database storing highly personal data (name, date of birth, passport information, biometric data) of more than 350 million individuals (Fig. 5.4).[47] This constitutes a substantial challenge to data protection standards and data security. The European Data Protection Supervisor (EDPS, see chapter 4.2.4) therefore sceptically voiced his concerns regarding CIR-sized ICT-systems.

[46] [Mon19]
[47] [Cim19]

However, he admits that current developments and issues in the areas of public security and border management require an adaptation of existing authority cooperation approaches and an intelligent utilisation of data already managed by these authorities.

Interoperability can be seen as a highly useful tool for the establishment of efficient and effective information exchange strategies, but it is essential to create new interoperability solutions with a strong focus on the protection and preservation of the fundamental right of EU- and non-EU citizens to privacy and correct handling of their personal data. Approaches like establishing CIR might, therefore, aid and facilitate public administration and increase safety for individuals, but since the three existing databases will be joint with three completely new databases, the ultimate consequences of this affair on fundamental rights of individuals are still unforeseeable and proper assessment of potential issues needs to be kept in mind.[48]

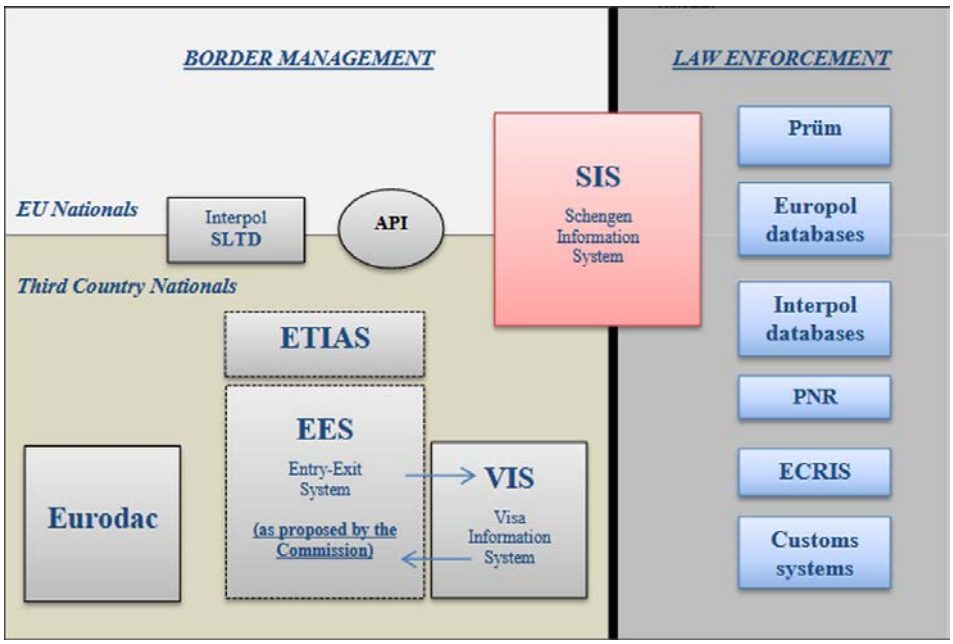


Figure 5.4: [Cim19] - CIR (Common Identity Repository).

[48] [Sup18]

CHAPTER 6

# Methodology of Police Data Exchange

As discussed in chapter 5, interoperability constitutes several layers that have to be equally considered and governed to improve efficiency and effectiveness. Regarding police data exchange, an essential and fundamental premise to ensure seamless and reliable transmission and usability of information is the optimisation of technological and methodological components. The ICT systems aiding police work have to be harmonised in regard to data formats, storage and transmission.

This chapter outlines standards for data structures and communication systems that are promoted for European police data exchange. It also introduces a range of information systems that are used on the European level (Europol) and in Austria (Federal Criminal Police Office, .BK).

## 6.1 Data Structures and Communication Systems

Communication between European authorities relies on a framework of XML-building blocks that can be interchanged and combined in standardised schemata to create functions for e-government applications. Recommendations for formatting conventions, interface specifications and implementation strategies are developed by designated ICT-task forces.

### 6.1.1 XML Data Format

XML is an acronym of eXtensible Markup Language and it is a text-based data format which can be used to establish hierarchic structures within a file. Structurally, XML encompasses a defined record of so-called tags that are marked by two arrow brackets (<, >), consist of a keyword (name) and a value, and can be used to mark down nested information, thereby creating hierarchy structures. Its use extends across a vast range of

applications that require the description, storage and exchange of data as well as the import and export of such data.[1]

For the purpose of e-government applicability, XML-schemata are drawn up to define the basic elements and datatypes used in the communication between authorities, that are complying with recommendations published by the World Wide Web Consortium (W3C), which is an international community promoting the standardisation of web content.[2]

### 6.1.2 Universal Message Format (UMF)

Hundreds of international and national data management systems[3] store and utilise similar information. Not only does this create redundancies, but it inhibits users from tapping the full potential of these databases, if only accessed individually. Since some of these systems have been established quite some time ago and developments in the ICT sector are rapidly evolving, their data formats are sometimes highly divergent and interoperability is weak.[4]

To cope with those shortcomings, the Universal Message Format (UMF) has been developed by Eurojust, Frontex, Interpol, Europol and the EU Financial Support in collaboration with 12 EU member states. It is supposed to constitute a new standard that European authorities are compelled to comply with.[5]

UMF can be seen as an XML "dialect" that has been tailored to fit the needs of a specialised niche of data exchange, as is the case for information that has to be shared between international police and judicial authorities. UMF-documents consist of UMF segments that are responsible for the structure of the file and UMF elements that constitute the actual XML tags and values, defining the data within those segments.[6]

In 2014, Europol defined UMF in a publication as "a set of concepts (building blocks) to construct standard data exchanges for interconnecting dispersed law enforcement systems"[7], in which UMF is not an internal structure of systems or databases, but acts as mutual interpreter that translates these internal specifications to a data format that follows standardized rules and can be transmitted and understood reliably across all participating systems. It serves as a "layer" between systems and international interfaces, as depicted in Fig. 6.1.

[1] [HM19]
[2] [Con18]
[3] [Eur14b, p. 2] - SIENA, EIS, AWF, I-24/7, iLink, SLTD, SMW, SIS-II, VIS, EURODAC, Prüm, EPOC, EUROSUR, etc.
[4] ibid.
[5] ibid.
[6] [Cen14]
[7] [Eur14b, p. 3]

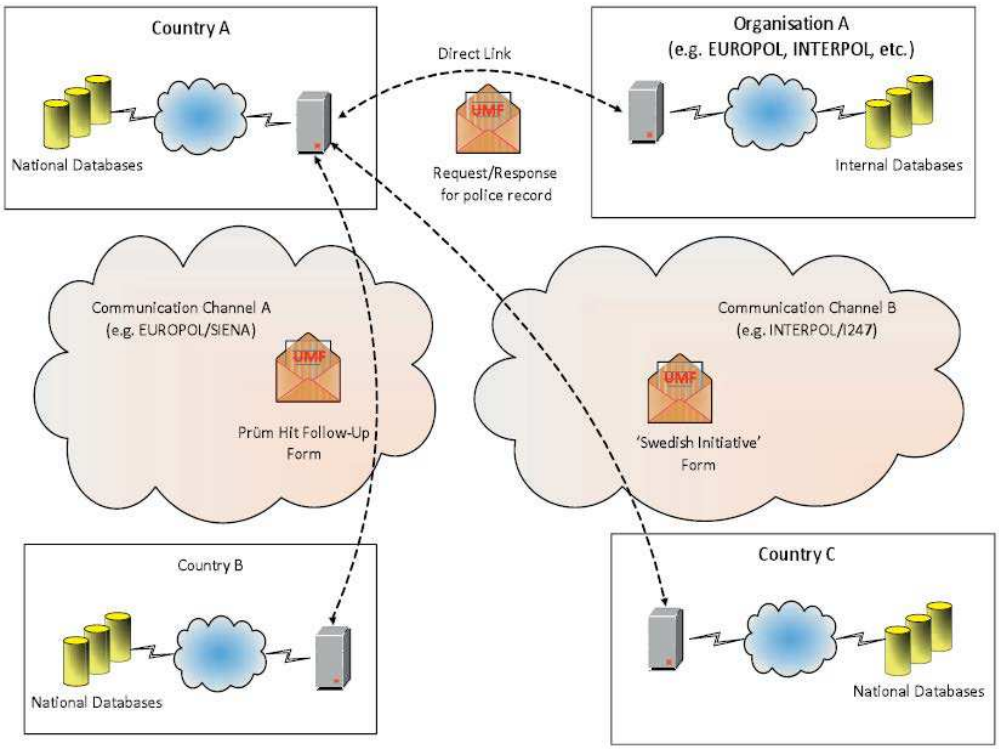


Figure 6.1: [Eur14b, p. 3] - "UMF as a layer between systems".

Europol lists the main advantages of using UMF as follows:[8]

- Shorter response times – due to faster and more reliable interpretation.
- Better decision making – due to reduction of ambiguity and clear standards that users are taught to understand.
- Improved data quality – due to easier cataloguing and referencing.
- Better case understanding – due to the reduction of language barriers and reduction of ambiguity.
- Better statistics – due to facilitated revision of exchanged data through improved traceability.
- Less ressources needed – due to all of the above, as well as the reusability of building blocks and designs for developers.

As of today, the system-independent UMF data and information exchange standard is broadly used by Europol and Frontex. For example, since 2014 inquiries for fingerprints

[8] [Eur14b, p. 5]

and DNA-data can be performed using a "UMF-compliant, multi-language, electronic form"[9], as designated for decentralised procedures in the Prüm Decisions (see chapter 3.1.8).

Under the administration of the German Federal Criminal Police Office, version 1.1 of the UMF 3 had been introduced in the scope of the UMF project action plan drafted in 2015.[10] It is now implemented as a Representational State Transfer (REST) service in 17 participating member states plus Norway, eu-LISA and Interpol. Europol uses this service in their newly established Querying Europol Systems (QUEST) database that is based on Europol's Secure Information Exchange Network Application (SIENA) and ensures encryption of data transferred between the Europol Information System (EIS) and national authorities (see chapter 6.2). However, so far only the five countries involved in the pilot project (Estonia, Finland, Greece, Poland and Spain) have access to EIS. Other countries have yet to implement the respective interface.[11]

### 6.1.3 Reference Model POLICE

POLICE is a reference model for international police data structures that was introduced by Europol. The acronym concludes the six most important and broadly used or cross-checked components of information that contribute data to a specific criminal or a surveillance inquiry: Person, Organisation, Location, Item, Connection, Event (Fig. 6.2).

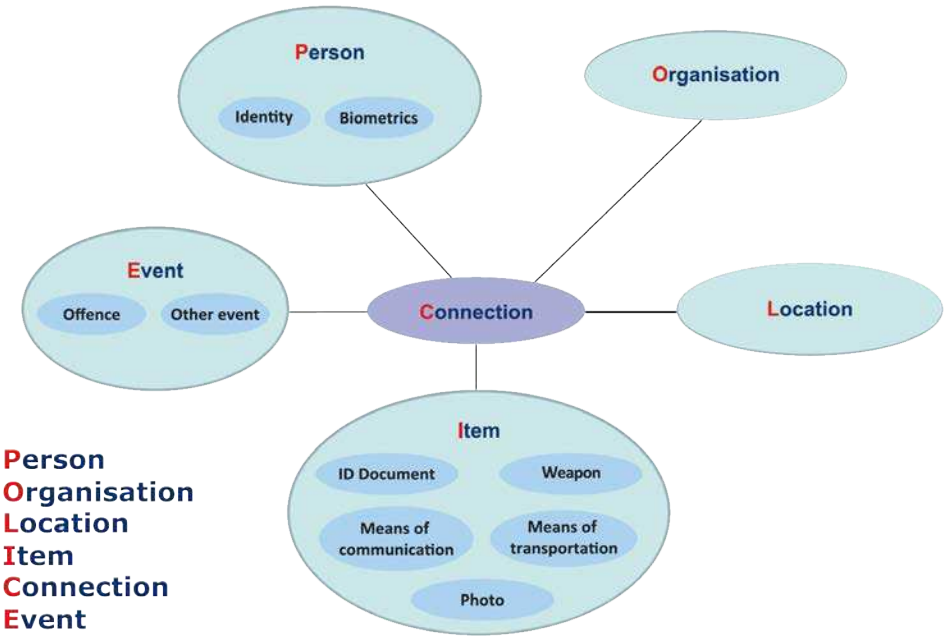


Figure 6.2: [Eur14b, p. 4] - "'POLICE' Information Model".

[9] [Mon18] - „UMF-konformes, mehrsprachiges, elektronisches Formular verwendet".
[10] [otEU16]
[11] [Mon18]

For each of these components developers and users are encouraged to use UMF building blocks to record data according to UMF rules and standards. This includes mapping the model to UMF by taking and transferring only the case-specific data necessary instead of the entire model. It also includes the identification of objects, relations and attributes that ensure reliable information exchange even if they are not covered in the standard, and to add these buildings blocks together and combine them to form a data pool with higher potential and an easy to navigate structure that improves accessibility at the same time.

### 6.1.4 Excursion: Digital Austria

With the last formation of the government in January 2018, the Austrian ministry of economics was renamed and is now known as the federal ministry for digitalisation and business location ("Bundesministerium für Digitalisierung und Wirtschaftsstandort", BMDW).[12]

To access up-to-date, first-hand information about the "Digital Austria" project, I sent a written inquiry to the head of the respective department "I/A/2 Internationale Beziehungen und Legistik", Mag. Peter Kustor. On May 7$^{th}$ 2019, Mr. Kustor's colleague DI. Dominik Klauser from the department "E-Government Bürger" contacted me via telephone and was so kind as to answer my questions.

Mr. Klauser informed me that the BMDW acts as coordinator and driving force for the digitalisation of Austria, while the responsibility for the implementation of recommendations and standards rests directly on the individual self-governing bodies (ministries, states, municipals etc.). The BMDW itself does not have legislative powers of assertion but relies on the decisions of the cabinet council.

The platform for the "Digital Austria" project resides within the BMDW. According to Mr. Klauser, Austria is leading the European field in regards to digitalisation of public administration and serves as an EU paragon for the adherence to the ISA$^2$ principles.

One example is that Austria employs a standard format interface specification called Electronic Data Interchange Akt (EDIAKT) II / Electronic Data Interchange for Documents (EDIDOC) for communication between a range of public institutions like police authorities, courts, public events and others. These institutions use electronic records and objects that differ due to manufacturer specifications and which are not standardised for business cases.

EDIAKT II combines single data file into uniformly manageable "EDIAKT-packages" that are structured in four hierarchical levels, starting with the "document", i.e. the original file in UMF, if it is not available in UMF, a standardised version has to be included. The smallest transferrable EDIAKT-package unit is the "business element" that encompasses one or more documents which can be combined with other business

[12] [dB19b] - (Bundesministeriengesetz 1986 – BMG): January 8$^{th}$ 2018.

elements to form a "business case". This again can be enveloped in the actual "(collective) business act". EDIAKT packages consist of:[13]

- Content data, the actual data values of a file (in standardised form).
- Meta data, describing the respective file to be transferred contextually.
- Process data, recording the processing instances and activities according to the XPDL-standard published by the Workflow Management Coalition (WfMC).
- Procedure-specific expert information that can be attached to any files.

To allow the seamless exchange of data, a transaction convention called "Elektronischer Akt des Bundes" (ELAK, translating to "Electronic Document of the State")[14] defines standards for the automated transfer of EDIAKT packages via web services. As central registries for electronic administration are continuously gaining importance, EDIAKT II as interface between different ELAK systems and its adjunct EDIAKT Viewer and Creator software in combination with the standard document format PDF/A serve as the main fundamental technology for long-term archiving of business acts.

The ELAK transaction convention aids with product-independent interface cross-linking of information systems to facilitate interoperability improvements and system integration. It builds on the following specifications:

- XML building blocks – The XML construction kit is a document drafted by the task force "communication architectures" that states organisational and technical guidelines for subject-specific XML data structures in electronic form. It provides elements that can be combined flexibly to create standardised applications for communication and information exchange between authorities. The specifications adhere to W3C standards and include XML structure models for business objects.
- XML "Eingangsprotokoll" (protocol for new entries) – This protocol is a standardised XML data set for ELAK processing that contains all data necessary for the cataloguing of a new business case according to the EDIAKT II structure (content values, meta data, process data, expert information).
- PersonData – The Person Data Record is a data set that inambiguously identifies a natural or legal person. It contains information like name, address, telephone number etc. and is used for all individual-related processes within the e-government.
- SOAP faults – The Simple Object Access Protocol (SOAP) standard is used for the communication between e-government applications. Messages are annotated with transfer data in the XML format and then relayed using established web protocols

[13] [Öst19b]
[14] [Öst19a]

(HTTP[15], SMTP[16]) that usually use specific error codes. SOAP faults (XML-sf) allows technically uniform handling of errors and the classification of errors in categories, thereby facilitating the identification of error sources.

During the phone interview, Mr. Klauser emphasised that SOAP and XML are still, due to their clear structure and hierarchy prioritised standards in the communication between authorities. He also informed me about the increasing relevance of JavaScript Object Notation (JSON) in combination with REST[17]. In the scope of the new Austrian Digital Office protocols like REST are promoted as the more reduced and efficient alternative, but SOAP is still broadly used and the access with older systems that still rely on it has to be ensured.

## 6.2 European and Austrian Police Information Systems

With the Treaty of Lisbon, Europol has been installed as an independent EU agency which fulfils the responsibilities of the European Police Office.[18]

However, already in the Europol Agreement from 1995[19] (ratified by EU member states in 1999) it was proposed that Europol is to implement and maintain a computer-based system to manage, access and analyse police data.[20] To this effect, The Europol Computer System (TECS) was created.

Its applicability was restricted to Europol's areas of responsibility: terrorism, illegal drug trafficking and human trafficking.[21] If at least two EU member states were affected by a case of this kind, Europol employed TECS for not only manhunt and search but also for investigative purposes. This differentiates TECS from the Schengen Information System (SIS) that was used for tracing operations only.[22]

Today, the Europol Agreement also includes updated regulations regarding police co-operation, tasks Europol with the responsibility for the technical and organisational maintenance of its information systems and determines which protocols for data storage, erasure and security Europol has to adhere to. TECS originally encompassed three individual systems. Of the three, the Europol Information System (EIS) and the Europol Analysis System (EAS) are still in use, but the Information Exchange System InfoEx has been replaced by the Secure Information Exchange Network Application (SIENA).

[15] Hypertext Transfer Protocol - Protocol for the exchange of data over a computer network.
[16] Simple Mail Transfer Protocol - Protocol for the exchange of e-mails.
[17] Representational State Transfer - Protocol for the exchange of information via networks.
[18] [PotC16c]
[19] [Heu07, p. 119]
[20] ibid., p. 118f.
[21] [PotC16c] - The complete list of international crime can be found in "Annex I - List of Forms of Crime Referred to in Article 3(1)" of the Regulation (EU) 2016/794.
[22] [Heu07, p. 119ff.]

Austria employs its own information system in the scope of the "Integriertes Polizeiliches Sicherheitssystem" (IPOS, translating to "Integrated Police Security System").

### 6.2.1 Europol Information System (EIS)

The European Information System (EIS) is a database that contains data of all criminal prosecution cases Europol and their cooperation partners are working on. The EIS is therefore the central information hub for all available data. Case files include information on involved or afflicted individuals, individual-associated vehicles, data on communication and financial flows regarding the case, identification documents and objects that were means to commit the crime (drugs, arms, currencies).[23]

Access to the EIS is restricted to the respective national offices of involved member states and their liaison officers, the director of Europol and their vice directors and authorised Europol officials via SIENA.[24] Other police units can request access to specified data via the Europol Operation Center (EOP).[25]

EIS entries are made by these just mentioned authorised individuals or Europol itself. Europol mostly feeds the systems with data from third countries (non-EU) or analytic reports, as the EU Council legal act from 1998 enables Europol to draft agreements concerning the data content with third countries.[26] However, cases of violation of fundamental human rights prosecuted in third countries are not allowed to be stored in the system.[27] The immense advantage of using EIS is the cross-linking of individual information, thereby creating an information network for the mapping of cases in a more comprehensive manner.[28] Since 2013 EIS includes DNA samples and data regarding cybercrime.[29]

Police data stored in the EIS has to be deleted immediately and irreversibly or corrected if a case is closed or the individual involved with the crime has been legally acquitted of the charges. The same applies to data that is not actively used and therefore serves no specific purpose. Only authorities who entered the data are authorised to erase, correct or alter it.

Adherence to the Europol regulations concerning police data storage, exchange and protection are monitored by the organisation's Data Protection Officer (DPO), the European Data Protection Supervisor (EDPS) and the national surveillance committees (see chapter 4.4).

According to the Europol Review 2016-2017, "395.357 of EIS objects are stored in the EIS (increase 34%) compared to 2015. Major crime areas related to objects are 21% to

[23] [Eur19k]
[24] [Eur13]
[25] [Eur19q]
[26] [Krö04, p. 49]
[27] ibid.
[28] [Eur13]
[29] [Eur13, p. 2]

drug trafficking, 18% to robbery, 14% to other offences in Europol's mandate, 7% related to fraud and swindling, 6% related to money laundering.".[30]

From 1996 to 2005, Austria paid approximately 1.5 million Euros for the development and implementation of EIS. In 2006, Austria added 2,636 entries to the database, pushing it to the 4$^{th}$ position in a ranking of all EU member states regarding data contribution. Between 2011 and 2013, however, only a small part of data was entered in the system and Austria became the state with the lowest number of data contribution (approximately 200-400 entries). This decline was due to the high time investment necessary. After a reprimand by Europol it is planned to invest into a data loader software to solve this problem.[31]

### 6.2.2 Europol Analysis System (EAS)

The Europol Analysis System (EAS) is a high-performance analysis tool for the strategical evaluation of data provided by EU member states and third countries.[32] 120 data analysts at Europol (eff. 2016)[33], a part of which is positioned at the EOP working with this system. The EOP is where the constant exchange of data regarding terrorism and organised crime between Europol and its operative partners in the area of criminal prosecution in administratively managed and operationally supported. The EOP also maintains a data-cross-checking-service to identify connected elements within the data exchanged and provided by the national offices, organisations and agencies subjected to public law or third countries. Information gathered from general or strategical analyses are subsequently condensed in analytic reports and provided to all member states by their liaison officers.[34]

With its integration points with EIS and SIENA, the EAS constitutes the technological platform for the deployment of Analysis Work Files (AWF) that can be created whenever at least two EU member states are affected by a crime to be investigated. Other member states can join the AWF on demand.[35]

By filing individual AWF, a closed analysis system that contains individual data combined in an overview-like "big picture" is created that aids in detecting context and relations. By doing so, it enables police officers to gain deeper understanding of a case and potentially facilitates predictions and conclusions drawn for the data, thereby improving criminal prosecution and control. AWF data is provided by the national offices[36] and can be of general, strategical or operational form.[37] They can contain information from evidence, opinions and personal estimations and be cross-linked between AWFs if necessary and

[30] [Eur17d, p. 71]
[31] [Rec17, p. 255]
[32] [Eur17d, p. 71]
[33] ibid.
[34] ibid.
[35] [Eur09, p. 29]
[36] [dB19d]
[37] [Krö04, p. 49f.]

relevant.[38] In addition to data concerning suspects or convicted individuals as defined in article 8 of the Europol Agreement, the AWF can also contain information on actual or potential witnesses or victims as well as the personal network or other individuals who might be able to contribute information about the investigated crime.[39] These and further information can be accessed by other institutions on demand via the EOP.

For each AWF an analysis group that consists of data analysts, Europol officials, liaison officers and experts from the member state that provide data and information to be analysed or is affected by the analysis, is formed.[40] Data analysts are authorised to enter data, other participants have reading access. An implementation order for each AWF is given by the administrative board, wherein the content and scope of the file is stipulated, along with specifications drafted by the member states that concern the parameters and conditions of the data transfer.[41] National offices have to announce a reason for each data transfer, with Europol determining the precision for data utilisation to be given in these proposals. Until the AWF is officially entered in the system, member states are responsible for the data,[42] they assess the reliability and accuracy of the information they provide,[43] and they are furthermore authorised to restrict access and erasure of the AWF's content.[44] Europol also evaluates the content of the AWF using already existing data and informs member states in the case of discrepancies. Changes of the content are subject to unanimous decision[45] and information added to an AWF has to be revised first for correctness and actuality by Europol officials.[46]

Adherence to the regulations regarding these data transfers is ensured by a common surveillance instance as well as by national authorities: "In addition to the joint supervisory body, each Member State designates a national supervisory body to ensure that personal data are input, retrieved and transmitted to Europol in accordance with national law. This body also ensures that the rights of the individuals concerned are not affected.".[47]

Similar to the regulations concerning EIS, data entered in the EAS is stored for three years. Annual revisions determine if the respective data is to be deleted. Permission to prolong the storage time frame by another 3 years can only be suggested by Europol's director.

The analytic reports that result from the information in the EAS help decision makers in identifying and prioritising actions to combat organised crime and terrorism:[48]

[38] [Heu07, p. 125]
[39] ibid., p. 124
[40] ibid., p. 125
[41] ibid.
[42] ibid., p. 126
[43] ibid., p. 125
[44] ibid., p. 126
[45] ibid., p. 125
[46] ibid., p. 126
[47] [EL09]
[48] [Eur19s]

- Serious and Organised Crime Threat Assessment (SOCTA) – serves for the evaluation of potential dangers from acute and current developments in various areas of criminal prosecution.
- Internet Organised Crime Threat Assessment (IOCTA) – supports authorities in taking action against organised cybercrime.
- EU Terrorism Situation and Trend Report (TE-SAT) – an annual report that lists failed, intercepted and closed cases of terrorism within the EU.
- Scanning, Analysis and Notification (SCAN) – Europol's early warning system for prognosis and timely identification of new threats of organised criminal activities.

### 6.2.3 Secure Information Exchange Network Application (SIENA)

As the successor of TECS' former indexing system InfoEx, the Secure Information Exchange Network Application (SIENA) is an electronic system to exchange operative information between EU member states and Europol.

InfoEx was operative from 1996 until 2009, when it was replaced because of the implementation of the first version of SIENA.[49] It was available for all liaison officers and authorised Europol officials in The Hague. Without the required clearance, users could still make inquiries to the system to learn if relevant information regarding a specific investigation were available in the database,[50] but without gaining knowledge of the content of the available data. Exchange of relevant data was performed via an encrypted and secured channel (Secure Sockets Layer (SSL))[51].

In the context of police cooperation, where sensible data that must not be intercepted has to be exchanged between Europol and national authorities, it is obligatory to use indexing systems that support a fast, reliable and secure transfer of information. The consequence of these requirements was the development of SIENA, a system that can be accessed by EU member states and third countries with an operational cooperation agreement.[52]

The EU-wide implementation and usage of SIENA was agreed on by police and terrorism specialists during the "Danziger Gespräche", a safety conference that has been held annually since 2000.[53] SIENA went online in July 2009.[54] It is able to translate inquiries from police institutions and authorities into 24 administrative languages and three alphabets.[55] To allow access for third parties a new version, SIENA 2.1, was installed in

[49] [Eur09, p. 8]
[50] [Eur, p. 21]
[51] [Bun18a, p. 2]
[52] [Eur18, p. 61] - Terrorism Situation and Trent Report 2018.
[53] [MV16]
[54] [Eur09, p. 10]
[55] [Bor08]

2011.[56] In 2015, the effective version of SIENA was SIENA 2.8[57] and an update to version 3.0[58] is planned. SIENA will thus obtain the security clearance level "EU Confidential"[59] and replace the former communication tool of the Police Working Group on Terrorism (PWGT) which has reached the end of its lifespan.[60] SIENA's data exchange is restricted by a maximum size of 50MB per file,[61] larger files are transferred separately via the Large File Exchange (LFE) system.[62]

With SIENA, a specialised sector for the combat against terror was created. Authorities working on terrorism control can now directly transfer information to Europol and other agencies, whereas before data regarding terrorism could only be indirectly exchanged as it had to take a detour via Europol's national or liaison offices.[63] Due to these developments and the establishment of facilitated, efficient transfer routes between Europol and the EU member states, the extent of information exchange concerning the combat against terrorism has peaked and reached its all-time high in 2016.

When the terrorism attack on the satire magazine Charlie Hebdo in 2015 made headlines worldwide, a cooperation between Europol and the task force "Fraternité" led to the exchange of high-value information and consequentially enabled the national police authorities to identify new suspects. In the timespan of a single year between the attacks and 2016, Europol's person-related data content has increased almost by tenfold[64] and the size of the data base concerning terrorism has almost doubled (from approximately 2,000 to almost 4,000 cases) in the same year.

The number of messages exchanged via SIENA also increased from approximately 56,000 to almost 95,000.[65] This is even surpassed by far by the operational messages exchanged between participants, as their number increased by 19% between 2015 and 2016 to an astonishing amount of almost 870,000 operational messages, 71% of which concerned robberies (17%), drug trafficking (15%), illegal immigration (15%), fraud (12%) and terrorism (12%).[66] Furthermore, the number of operations with focal points supported by the European Counter Terrorism Centre (ECTC)[67] increased from 86 to 127, with a yield of confiscated arms and explosives of 42,000 and almost 83,000, respectively. In the field of terrorism, Europol's European Union Internet Referral Unit (EU IRU) majorly contributes to the combat against terrorist propaganda. The unit, which assembles a range of experts on religiously motivated terrorism, interpreters, ICT experts and police

[56] [Eur12, p. 2]
[57] [Cou16, p. 6]
[58] ibid., p. 7
[59] [Mon16]
[60] [Cou16, p. 7]
[61] [Eur16d, p. 42] - Europol Review 2015.
[62] ibid.
[63] [Eur18, p. 61]
[64] [Eur17d, p. 30] - Europol Review 2016-2017.
[65] ibid.
[66] ibid., p. 69
[67] [Eur19j] - European Counter Terrorism Centre.

officers has reported over 51,000 (eff. 2017) cases of terrorist online content, with a 84.8% success rate at taking down and erasing the respective content.[68]

Overall, more that 46,000 SIENA cases were initiated in 2016, which constitutes an increase by 16% in comparison to 2015, with 84% of these cases were issued by EU member states, 11% by third countries, and 5% appointed directly by Europol.[69]

In January 2018, the EAS registered over a million of operational messages, derived from users in 47 countries and 1,200 authorities.

In his September 2018 speech concerning the situation of the union, EU Commission Director Jean-Claude Juncker stated: "Europeans rightly expect their Union to keep them safe. This is why the Commission is today proposing new rules to get terrorist content off the web within one hour – the critical window in which the greatest damage is done."[70], thereby emphasising the necessity of state-of-the-art developments for police data exchanged.

### 6.2.4 Schengen Information Systems (SIS)

The Schengen Information System (SIS) is a technical cooperation system and a computer-based manhunt and information system within the state union of the Schengen area.[71] Currently, 46.5 million SIS files are used by 26 Schengen countries, Ireland and Great Britain, and non-EU countries Iceland, Norway, Switzerland and Lichtenstein. The system was implemented as the centerpiece of compensatory measures of the efforts to remove the necessity of border controls at domestic borders within the Schengen area.[72]

The SIS II is split into two parts:

The central Schengen information system (C-SIS) which is in Strasbourg and the nation Schengen information systems that is used in the individual member states (N-SIS). Other than the Automated Fingerprint Identification System (AFIS), SIS only provided "weak data", which excludes biometric data. However, the system's capacities were exhausted in the scope of the EU expansion process, and a new version, SIS II, was implemented.[73] Since 2013, SIS II now offers the opportunity to process biometrical data.[74]

SIS II constitutes an expansion of the original manhunt and search system to an investigative tool where information concerning a suspicious individual can be cross-checked with information on other individuals and objects. Originally, it was planned to implement the new system in 2007, but it took officials until 2013 to eliminate all coding problems (10,000 input errors, no emergency back-up plan).[75]

[68] [Eur18, p. 62]
[69] [Eur17d, p. 69]
[70] [Com18b] - President Jean-Claude Juncker: "State of the Union Address (2018)".
[71] [Feh01, p. 45]
[72] ibid.
[73] [Com13a]
[74] [Com13b]
[75] [Bor13]

Today, the European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA), which was launched in 2012, is tasked with the day-to-day running of the SIS II[76] and also the administration of the VISA information system VIS and the fingerprint database EURODAC.[77]

SIS II is subject to very strict data protection regulations and operates under a rigorous surveillance of a common supervisory body and the national authorities working in the Supplementary Information Request at the National Entries (SIRENE) offices.[78] Effective 2013, the system processed approximately 50 million search and manhunt files concerning individuals and objects.[79]

### 6.2.5 Europol Platform for Experts (EPE)

The Europol Platform for Experts (EPE) is a secure web platform for collaborating experts from different criminal prosecution areas. It facilitates the exchange of established procedures and techniques as well as documentation of case studies for the purpose of combating crime.

The platform provides tools and communication infrastructure and allows experts to directly interact with each other in a secure environment via private messages and forums.

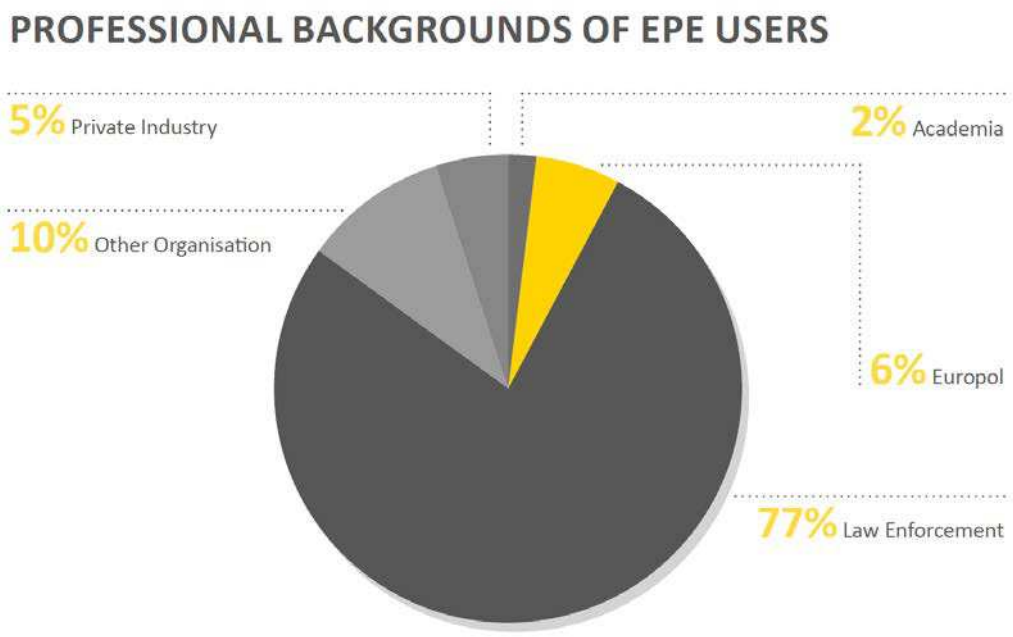


Figure 6.3: [Eur17d, p. 72] - Professional Backgrounds of EPE Users.

[76] [EL14]
[77] [Uni16a]
[78] [ÖD19]
[79] [Rec17, p. 256] - Rechnungshofbericht zum Bundeskriminalamt 2015.

In 2016, EPE had over 10,000 users from 85 countries, 2,700 of those joined EPE in the year 2016 alone. As depicted in Fig 6.3, the 2016 annual Europol review states that 77% of EPE users came from a law enforcement professional background. Users from Private Industry and Academia made up 5% and 2% respectively. (Fig. 6.3)

EPE members are now also provided with the aforementioned LFE for files larger than 50MB that cannot be transferred via SIENA directly. Furthermore, they are provided with the Europol Malware Analysis Systems (EMAS) used in the area of cybercrime. Both use the platforms EPE Central Authentification System (EPE CAS) to monitor and identify all users.[80]

Additionally, EPE took over the administration of the centralised European Union Bomb Data System (EBDS)[81] database which contains information related to explosives, the Synth Lab and the Cocaine Logos.[82]

Examples of EPE communities are:[83]

- ATLAS – a network of special forces focusing on intervention and combat against terrorism, founded after the terroristic attacks on the World Trade Center in New York on September 11$^{th}$ 2001.
- The European Network of Forensics Science Institutes (ENFSI) that was founded recently to promote quality and competence management, research and education.
- ROVER – a community providing an overview of the Passenger Name Record (airlines storing information on their customers for administrational reasons) legislation and its regulations.

### 6.2.6 Austrian Police Information Systems

As discussed in chapter 3.2.5, the Austrian Federal Criminal Police Office ("Bundeskriminalamt", .BK) serves as a central hub for all criminal prosecution and police cooperation. In the scope of the Digital Austria project, the .BK is therefore an important focal point in the context of electronic information transfer and police data exchange.

Over the last years, Austria already invested a lot in education and higher education of police officials to combat fraud and white-collar crime. New modules for the respective investigators were launched in May 2017.[84]

[80] [Eur17d, p. 72]

[81] [Com17a] - "European Bomb Data System (EBDS) is an IT platform which allows Member States to share timely and relevant information and intelligence on explosives and CBRN materials and related incidents. Since it requires a higher level of secure connection, Europol created a complementary on-line-based Europol Platform for Experts, where users can interact and collaborate with each other via virtual communities.".

[82] [Eur17d, p. 72]

[83] ibid.

[84] [Bun18b, p. 23] - Polizeiliche Kriminalstatistik (PKS).

According to their motto, which translates to "think, plan and act internationally"[85], executive officers will be commissioned for international police work so that investigations beyond the country's borders so that individuals that committed crimes in Austria will be held accountable regardless of their residency.

The annual criminal statistics report for 2017 that was published by the BMI states that the Prüm Agreements will be expanded across Southeastern Europe and that databases will continue to be cross-linked, not only within Austria, but also with their pendants on EU-level, hereby mentioning the importance and necessity of interoperability of the Austrian systems with the European counterparts.[86] To enhance the capabilities of the .BK, technical applications and tools that facilitate routine police work will be promoted strongly over the next years. Together with exact analytic programs these tools should help authorities and individual police officers to increase their efficiency and investigation success and in specifically addressing a variety of focal points. In 2018, an application for facial recognition was implemented. Digital analytic systems for crime scene traces, firearm traces and suspect material in regard to child pornography and human trafficking will be provided in the future. Additionally, mobile hardware like smartphones and tablets will enable police officers to apply these technologies on site.[87]

#### 6.2.6.1 "Integriertes Polizeiliches Sicherheitssystem" (IPOS)

The project "Integriertes Polizeiliches Sicherheitssystem" (IPOS, translating to "Integrated Police Security System") was launched in 2011 and is planned to implement the system in all security executive offices in agreement with BAKS-4 facilities.[88] Technical systems supporting IPOS were purchased and 300 employees got tasked with tailoring them according to the needs and functionality of the Austrian police system.

Elements of IPOS are the "Integrierte Kriminalpolizeiliche Datenanwendung" (IKDA, translating to "Integrated Ciminal Police Data Application"), the "Protokollieren-Anzeigen-Daten" (PAD, translating to "Protocol-Indication-Data") and the "Zentrale Datensammlung" (ZDS, translating to "Central Data Collection").[89]

#### 6.2.6.2 IKDA, PAD and ZDS

IKDA is a system for police record administration and storage that the Austrian Ministry of the Interior ("Bundesministerium für Inneres", BMI) had proposed already in 2001, but which was developed and implemented in 2011 and 2014 respectively. The delay mainly resulted from the highly specific requirements posed by criminal police work that could not be fulfilled by the "Elektronischer Akt des Bundes" (ELAK, translating to "Electronic Document of the State").[90] It was implemented for the processing of national

[85] [Bun18b, p. 23] - "International denken, planen und handeln".
[86] ibid.
[87] ibid.
[88] [Nos04] - Öffentliche Sicherheit: Das Magazin des Innenministeriums 7/8 2014.
[89] ibid.
[90] [Öst19a]

and international data and subsequent analysis to optimise and improve procedures in criminal investigation and prosecution.

PAD is a module that was conceptualised solely as documentation system for incoming case files. Police offices entered data about investigations and reported offences, but the .BK and State Offices of Criminal Investigation (Landeskriminalamt, LKA) did not have direct access.[91] Due to the server structure and the vast number of files (88 databases containing approximately 30 million case files) the system was comparably slow and was soon replaced by the "Protokollieren-Anzeigen-Daten - Next Generation" (PAD NG). The new system was developed by external contractors and the BMI. Still, while being implemented to facilitate the initial input process for users, it was not designed to be an actual information system due to data protection reasons.[92]

Ultimately, the "Zentrale Datensammlung" (ZDS, translation to "Central Data Collection") is to replace the former "Elektronisches Kriminalpolizeiliches Informationssystem" (EKIS, translation to "Electronic Criminal Police Information System") and will access the data stored via new user interfaces and newly established cross-links between data to accelerate the response to high throughput inquiries.

#### 6.2.6.3 Security Monitor

The Security Monitor ("Sicherheitsmonitor", SM) is a central database that serves as an early-warning system and criminal threat assessment tool. It was implemented by the .BK in 2004 and has since been continuously advanced. Essential cornerstone data on all intentional criminal offences are integrated automatically from PAD, a change in PAD data therefore transfers directly to the SM, and its contents are accessible for all executive forces online. The .BK uses the SM to compile daily reports on for example high priority offences, basic statistics that are distributed automatically to all LKAs.

The analytic department within the .BK also uses the SM to continuously monitor threshold transgressions within a range of investigative areas like robberies, and issues its own reports on an Austria-wide and an individual state level. Situation reports concerning specific forms of criminal activities are made accessible via the BMI's analysis platform for all decision makers. Furthermore, in cooperation with the Joanneum which is a Research Community residing in Styria, Austria, statistical models were generated to evaluate criminal developments in specified areas.[93]

#### 6.2.6.4 "Factotum" Databases

An additional and probably obsolete tool that is in dire need of revision for the operative analysis of criminal activities are the .BK's so-called "Factotum" databases where investigators gather and manually structure information regarding case files on a voluntary

[91] According to BMI: different safety authority responsibilities.
[92] [Rec17, p. 236]
[93] ibid., p. 238ff.

basis, as there is no automated integration of PAD. The cross-linking on these information is supposed to provide a clearer overview and allows inquiries.

In 2014, 13 of these Factotums (regarding human trafficking, prostitution, narcotics etc.) were installed on demand from investigators. However, the manual input and cross-linking proved to be highly time-consuming.[94]

[94] [Rec17, p. 247]

CHAPTER 7

# Impact and Success of European Police Cooperation

The final chapter of this work addresses the achievements of European police cooperation.

First, an overview of select European Police Cooperation projects is given, and ultimately the Austrian situation and impact of the Europeanisation of police work on various aspects of Austria's security and public administration are discussed.

## 7.1 Select efforts of European Police Cooperation

Europol has published a list of its most noteworthy operations on the organisation's website. The operations are chosen according to their respective characteristics, as for example:[1]

- The European Joint Unit on Precursors (EJUP), crime field drug trafficking, "first Joint Investigation Team (JIT) in Europe" (2002)
- Operation Shovel, crime field money laundering, "first ever mobile office deployment" (2010)
- Operation Oakleaf, crime field organised property crime,"first ever operation to crash our secure communication network due to the high volumes of contributions received" (2012)
- Operation Veto, crime field sports corruption, "highest international media attention"

[1] [Eur19l]

- Joint Operational Team Rose of the Winds, crime field drug trafficking, “biggest operation in this crime field”
- Operation Alphabay/Hansa, crime field cybercrime, “most sophisticated cyber takedown”

To perform these operations, Europol and the EU employ a range of strategies, of which three are presented here.

### 7.1.1 European Crime Prevention Network

The European Crime Prevention Network (EUCPN)[2] was founded in 2001 by the EU Justice and Internal Affairs Council. The goal of implementing this network is to advance a range of approaches in the area of crime prevention on EU level, with a predominant focus on juvenile delinquency, crime in metropolitan areas and drug trafficking. EUCPN therefore collects information on successfully established measures and techniques for crime prevention that are provided by EU member states.

Besides operating on all three namely the local, national and European level, EUCPN also launched initiatives and campaigns for common awareness of criminal threats for citizens. It also invests in education and training of police officials to sensitise for crime prevention issues and crime opportunities.

### 7.1.2 Joint Investigation Teams

Following the June 2002 Council decision 2002/465/JI[3], Europol member states can now form Joint Investigation Teams to address particular issues:

“A joint investigation team is an international cooperation tool based on an agreement between competent authorities - both judicial (judges, prosecutors, investigative judges. . . ) and law enforcement - of two or more States, established for a limited duration and for a specific purpose, to carry out criminal investigations in one or more of the involved States.”[4]

A JIT, therefore encompasses at least two representatives of police and judicial authorities from the respective member states or Europol. However, while Europol can provide a substantial amount of support and resources, its participation in a JIT is not obligatory and the team can also be formed between national authorities only.[5] In any case, the JIT is supported by Eurojust’s JIT network secretary office in The Hague.

Two major advantages of JITs are that they enable investigators to directly exchange information and data, circumventing the comparably tedious route via mutual legal

[2] [EUC19]
[3] [otEU02b]
[4] [Eur19p]
[5] [Eur19n]

assistance agreements. Furthermore, seconded members from other countries than the state the JIT operates in or even from non-police and non-judicial background that might benefit the investigation can be present and participate.[6]

As JITs constitute a temporally and topically defined structure of police cooperation, there are clear regulations on their closure and the evaluation of a JIT's output after it has been terminated is encouraged strongly.[7]

### 7.1.3 EMPACT Platform

In 2010, a 4-year policy cycle was initiated by the EU Council to strategically combat the most imminent and major criminal threats in the EU. Cooperation and coordination were considered key elements to maximise success in criminal prosecution and crime prevention.[8] The policy cycle was renewed twice from 2014 to 2017 and from 2018 to 2021 and was enforced in the scope of the European Multidisciplinary Platform Against Criminal Threats (EMPACT) project.[9]

The last policy cycle from 2014 to 2017 focussed on the following crime fields:[10]

- Facilitation of illegal immigration.
- Human trafficking (including exploitation of workforce and sexual exploitation).
- Manufacture and distribution of counterfeit and substandard products that violate the regulations in the health, safety and food sectors.
- Excise duty and Missing Trader Intra-Community (MITC) fraud.
- Synthetic drug production and trafficking.
- Illicit trafficking of cocaine and heroin.
- Cybercrime (including credit card fraud, sexual abuse of children online and attacks on critical EU infrastructure and information systems).
- Illicit trafficking of firearms.
- Organised property crime (by criminal groups).

The current policy cycle from 2018 to 2021, however, is centered more on international crime.[11] While the focal points regarding counterfeit and substandard products, synthetic

[6] [Eur19n]
[7] ibid.
[8] [otEU14, p. 2]
[9] [otEU19a]
[10] [otEU14, p. 5]
[11] [Eur19h]

drug production and the illicit trafficking of cocaine and heroin are integrated in other areas and not mentioned as individual priorities anymore. The list now also includes:[12]

- Environmental crime (specifically wildlife and illicit waste trafficking).
- Criminal finances and money laundering.
- Document fraud.


Figure 7.1: [Eur19i] - EU Policy Cycle.

To realise the policy cycle strategy from 2018 to 2021, Europol proposes a circular 4-step model, as depicted in Fig 7.1:

1. Employing the Serious and Organised Crime Threat Assessment (SOCTA) program to analyse current and future threats concerning the EU and help with the prioritisation of different crime fields.

[12] [otEU18a, p. 5]

2. Appraisal of the recommended priority choices performed by the Committee on Operational Cooperation on Internal Security (COSI). The EU member states' ministers for internal security and justice subsequently develop strategies on the foundation of this assessment. The resulting Multiannual Strategy Plan (MASP) has to be condoned by COSI.

3. The core operating range of EMPACT is the implementation of annual Operational Action Plans (OAP), which are tailored to the prioritised crime fields in project groups for each challenge. EMPACT support managers at Europol contribute to the projects in regards to organisation and logistics. The execution of each OAP is lead by representatives of the EU member states, who are responsible for biannual reports that are to be sent to the EMPACT supporting unit. There, progress and actions are supervised and approved by COSI.

4. Evaluation of the success and potential adaptions and adjustments in regards to prioritised crime fields is performed by COSI. This is based on the annual reports compiled by Europol from the information gathered on the individual OAPs and the independent assessment provided by the EU Commission. The results serve as a resource for the new policy cycle.

In May 2019, I could conduct a telephone interview with Mag. Elisabeth Hamidi,[13] who is the Head of the Europol National Unit. According to her, the success and impact of European police cooperation on Austria are most perceptible in EMPACT projects and their Joint Action Days (JAD)[14].

In 2018, EMPACT organised 8 JADs, of which each poses a short-termed high-intensity cooperation of approximately 5 days, and achieved outstanding results:[15]

- 1,026 investigations were initiated.
- Approximately 1.4 million Euros were confiscated from criminals.
- 1,137 suspects were arrested.
- 337 victims of human trafficking, 52 of which were minors, were identified.
- 207 firearms, 730 kilograms of heroin, 92 kilograms of cocaine, over 13 kilograms of cannabis and tobacco each, 5.5 kilograms of amphetamines and 2,500 liters of alcohol were confiscated.

Commenting on the results of the JADs 2018, Europol's executive director Catherine De Bolle stated:

[13] Head of the Europol National Unit - Office II/BK/2.2.
[14] [Eur19o]
[15] [Eur19h]

"I am very pleased to see this year's results of the Joint Action Days 2018. They are more than just numbers and figures, as they clearly show how successful strategically planned international cooperation with strong partners can be. The EMPACT priority crime areas are the major crime threats facing the EU and the Joint Action Days involve complex international investigations. Every day we at Europol strive to provide analytical and operational support to the Member States in combating his kind of international and organised crime."[16]

## 7.2 Police Cooperation with and within Austria

As discussed in earlier chapters, police cooperation in Austria is inherently dependent on the Federal Criminal Police Office ("Bundeskriminalamt", .BK), which is the central axis of information and data exchange in the security sector.

On an international level, Austria participates in the Schengen Information System (SIS) via its national Supplementary Information Request at the National Entries (SIRENE) office and communicates with Europol via liaison officers in The Hague.

### 7.2.1 European Impact on Austrian Police Administration

Europeanisation affects all parts of Austrian politics, therefore its impact on domestic affairs, internal security and the Austrian police is of course reflected in intranational police cooperation as well as the country's international relations.

The supreme goal of the Austrian doctrine of defence and security is to push the country towards the world's top ranks when it comes to safety and quality of living. Within the framework of a political union the individual state's role in questions regarding security becomes less substantial in general. International organisations and collaborators, as well as the state's administration, have to be able to rely on the European Union legislative to ensure the security of all member states and regulate international solutions.[17]

#### 7.2.1.1 Crime Prevention

As mentioned earlier (see chapter 7.1.1), the European Crime Prevention Network (EUCPN) is a network to develop and research approaches for crime prevention using information gathered from member countries.

On the national level, these approaches are employed in the form of a three-layered strategy to prevent criminal activities:[18]

- Primary crime prevention describes the promotion of ethical values and merits, it includes the training of non-violent problem solving strategies in kindergartens and

[16] [Eur19h]
[17] [fI17, p. 11]
[18] [BdI18]

schools to antagonise the general emergence of criminal energies in our society from a very early age on.

- Secondary crime prevention focuses on the prevention of opportunities that criminals could exploit, this classically comprises padlocks to secure objects and vehicles, alarm systems, or the alerting of neighbours during vacations to watch out for suspiciously behaving individuals.

- Tertiary crime prevention becomes effective when offences have already been committed. It encompasses strategies to prevent repetitious delinquency by measures like providing education and job training during the execution of a prison sentence as well as programs regarding resocialisation and integration of former convicts.

The .BK as Austria's central police cooperation hub serves as central unit for the coordination of prevention activities. Office II/BK 1.6 has even been set up specifically for this purpose. The State Offices of Criminal Investigation ("Landeskriminalamt", LKA) also have adjunct offices for crime prevention, and each police station has crime prevention specialists that were specifically trained for this purpose. Financially, the employment of preventative measures accounted for 4 million Euros or 0.57%-0.58% of the budget of the BMI for 2011 and 2012.[19]

The Austrian crime prevention advisory board comprises 4 members from 4 ministries (Internal Affairs, Justice, Women's Affairs, Economy). The chancellor's office ("Bundeskanzleramt", BKA) and the municipality MA 11 for Adolescents and Family are associated with it as well. Additionally, the board is joined by non-profit associations ("Verein Neustart", "Verein Tamar", "Verein Autonomer Österreichischer Frauenhäuser") and the domestic violence sanctuary "Gewalt in der Familie".[20]

#### 7.2.1.2 European Police Cooperation Act

Even before the Treaty of Lisbon, in which Europol was made an independent EU agency, Europeanisation of police cooperation has had an impact on Austria and all member states.

As it is a requirement for effective international police cooperation to optimise coordination and integration of differential legislatives, liaison officers were employed to improve communication and networking between the respective authorities. A priority is the containment of threats posed by internationalised criminal activities. Implementing early-warning systems and creating the infrastructure for facilitated exchange of data, information, and expertise was necessary.[21]

[19] Parliamentary question by Johann Maier to Johanna Mikl-Leitner, Federal Minister of the Interior, December 2011 - "Kriminalitätsprävention in Österreich" (9378/AB).

[20] ibid.

[21] [Arc09] - Archan 2009.

To this effect, Austria's Police Cooperation Act ("Polizeikooperationsgesetz", PolKG) was modified and integrated with European regulations in 2010. The new version is now called the EU-PolKG[22] and specifies cooperation regulations and general relations between Austria, Europol, and other EU member states. It covers all areas of law enforcement and applies to all domestic and foreign agencies that are operating within these areas (security, criminal prosecution, immigration and border control).[23]

The EU-PolKG replaces the formerly installed Europol agreement by which all legal acts of Europol had been adopted into Austrian national law, but much like the original PolKG, it still serves as foundation and guideline for bilateral agreements with other countries. It integrates contracts on other international relations like the Prüm Agreement or the Schengen Information System (SIS).[24]

Therefore, the second part of the EU-PolKG concerns existing structures, like the authorisations and working procedures of liaison officers, the National Security Agency (NSA)[25], the input and transfer of data, access to the Europol Information System (EIS) and other regulations that have already been stipulated in the former Europol Agreement.

The National Office was appointed as the bidirectional interface handling international police collaborations between Austria and Europol. This includes regulations regarding the authorisation for access to the Visa Information System (VIS) and the transfer of all data obtained from European and national information systems to third party countries.[26]

The result of these efforts is a law that facilitates direct interaction between authorities, thereby accelerating decision making and the approval of these decisions, which can now be flexibly adjusted to Europol's requirements.

#### 7.2.1.3 Internal Security and Criminal Prosecution

Europol is now responsible for transnational prevention and control of serious crime, terrorism and other forms of organised crime. The Austrian National Office is authorised to perform automated DNA profile searches and inquiries regarding fingerprint data and national registers on vehicle licences and to use the data obtained from Europol databases to support and enforce cross-border investigations.[27]

These authorisations regarding foreign territory are an important aspect of international police cooperation. With the EU-PolKG, foreign police authorities can employ their executives for law enforcement operations on Austrian territory. Examples of these operations are long-term transnational observations in which an individual who is under observation in an EU member state locates to Austria and is continuously observed by foreign authorities on Austrian territory. The immediate pursuit (hot pursuit), which

[22] [dB19c]
[23] [Lit10, p. 151]
[24] [Arc09]
[25] [Dic19]
[26] [Lit10, p. 152]
[27] [And10, p. 90] - Andre 2010.

refers to operations in which an individual is suspected to commit further crimes in Austria and is therefore prosecuted by the respective foreign law enforcement authorities is another example. In cases like these, Austrian authorities are obliged to respond to a request for mutual assistance and support their cooperation partners. Mutual assistance is granted by the minister of internal affairs, who is to be notified immediately after the request has been received. However, in cases in which domestic agencies directly border to foreign agencies who request mutual assistance, as well as in cases of imminent danger, the respective domestic unit is responsible for granting immediate mutual assistance on the spot.[28]

In 2018, Austria signed an agreement in The Hague that regulates the joining of forces between Europol and ATLAS, which is a network of 38 special forces distributed across 28 EU member states and associated countries (Switzerland, Norway, Iceland).[29]

In conclusion, the commitment of national law enforcement procedures to European standards and regulations requires adaptation of the national legal status and the integration of national decision making structures with European legislative via agreements and regulations. Under the condition that Austria is granted the right to be heard and the right to contribute actively to the process of legislation changes and innovations, EU legislation is given precedence over national law.[30]

### 7.2.2 Excursion: .BK Audit Report 2015

In 2015, the Austrian Court of Audit published a report on the .BK, taking apart its efforts to fulfil the requirements and challenges posed by the government. The following quotes are translated from German as literally as possible.

The audit court first criticised that "The .BK does not provide operating numbers concerning human resource dimensions and distributions"[31], and that it was "lacking the fundamental basics to evaluate and distribute staff resources under consideration of strategic focal points and core responsibilities of the organisation. The organisational plan developed by the .BK was not in agreement with the legally sanctioned personnel plans."[32]

In detail, the report stated that "The .BK was not able to fulfil its priority strategical task – the combat against complex forms of criminal activity in the fields of cybercrime and white-collar crime as well as organised crime – because it failed to redistribute its human resources accordingly. Although the actual number of personnel available to the .BK in the year 2014 amounted to 602 employees (including duty assignments)

[28] [Arc09, p. 62]
[29] [fI18b]
[30] [dB19c]
[31] [Rec17, p. 179] - "Das Bundeskriminalamt verfügte über keine Kennzahlen zur Personalbemessung und Verteilung".
[32] ibid. - "fehlten die Grundlagen, unter Bedachtnahme auf die strategischen Schwerpunkte und Kernaufgaben die Organisation zu evaluieren und Personalressourcen zuzuteilen. Der vom Bundeskriminalamt erstellte Organisationsplan war nicht auf den gesetzlich genehmigten Personalplan abgestimmt.".

and therefore substantially exceeded the required quota (518), operations performed in September 2014 were lacking 55%, 14% and 27% of the personnel deemed necessary by the .BK in the field of cybercrime, white-collar crime, and international task fulfilment, respectively. Additionally, the current system employed for the implementation of special task forces in the area of white-collar crime was resource- and time-consuming, and therefore inefficient."[33]

Other issues pointed out by the report were:[34]

- The "Protokollieren-Anzeigen-Daten" (PAD, translating to "Protocol-Indication-Data") system, supposed to serve as information interface between .BK and the individual LKAs was not installed. As a result, investigations were even more delayed due to the lack of immediate, direct accessibility of police data and subsequently increased administrational expenses.
- Lack of focus on the .BK's core responsibility: new and complex forms of criminal activity, namely cybercrime, white-collar crime and other organised criminal activities. Deficits in the implementation of appropriate strategies and procedures were detected to be the result of ineffective personnel and organisational structures, as for example some standardised educational programs in the area of cybercrime were missing.
- In 2013, the .BK presumably initiated new developments within the organisational sector without cross-checking the planned innovations with the federal personnel plans. The core elements of the restructuring process regarding a cybercrime competence center (C4) and the replenishment of the SIRENE office in the scope of the Schengen expansion could not be fulfilled.
- The .BK had participated in international projects and contributed experts, but the criteria on which these experts were chosen were incomprehensible and intransparent.
- The personnel deficit of 55% in the area of white-collar crime lead to inhomogeneous levels of qualification amongst the assigned human resources.
- Due to the lack of various technologies and expertise, the high data load accompanying large-scale operations could not be handled by the .BK and expensive

[33] [Rec17, p. 179] - "Das Bundeskriminalamt konnte seine prioritäre, strategische Aufgabe — die Bekämpfung komplexer Kriminalitätsformen im Bereich der Cyber– und Wirtschaftskriminalität sowie der Organisierten Kriminalität — nicht wie geplant erfüllen, weil das Personal nicht entsprechend umgeschichtet worden war. Obwohl der Ist-Personalstand des Bundeskriminalamts im Jahr 2014 mit 602 Personen (inklusive Dienstzuteilungen) deutlich höher war als der Sollstand (518), fehlten im September 2014 bei der Bekämpfung der Cyberkriminalität rd. 55%, bei der Wirtschaftskriminalität rd. 14% und im Bereich der internationalen Aufgabenerfüllung rd. 27% des vom Bundeskriminalamt für erforderlich gehaltenen Personals. Zudem war das derzeitige System der Einrichtung von Sonderkommissionen im Bereich der Wirtschaftskriminalität ressourcen– und zeitaufwändig und damit wenig effizient.".

[34] [Rec17]

external specialists had to be hired. Although a task force was entrusted with the search and product decision regarding appropriate management and analysis software already in 2012, no progress has been made in this direction.

- The implementation of an electronic administration system for case files took 10 years.
- The Security Monitor (SM) developed by the .BK as an early-warning system of current criminal threats caused increased processing expenses due to the high number of input errors that made up 16% of all entries and had to be debugged. This was mainly problematic because it resulted in delays concerning the acquisition of criminal offences with gaps of up to 7 days between the time of the crime and its capture in the SM system.
- The national data and information exchange via a Single Point Of Contact (SPOC) was considered appropriate. However, international exchange of data and information was criticised: Only a small part of available information was fed into the Europol Information System (EIS), although the implementation of the database interface had cost approximately 1.5 million Euros.
- The Schengen Information System (SIS II) and the Interpol communication system I-24/7 were only used sporadically or not at all.

In a follow-up audit report compiled in 2017, the audit court states that out of 19 recommendations given to the .BK in 2015, three have been realised completely, seven have been realised in parts, and nine have not been realised at all.

The situation regarding the international exchange of data and information has improved only marginally and gradually. To this date, data has to been entered manually into the EIS, and the data loader necessary for automating this process has not been implemented yet in expectation of new developments at Europol. Still, the object input was increased by almost 10% (417 to 449 within the timeframe from the first quarter of 2014 to the second quarter of 2015).[35]

[35] [Rec18] - Der Rechnungshof: Bundeskriminalamt - Follow-up-Überprüfung 2018.

CHAPTER 8

# Conclusion

This work addresses existing police cooperation approaches between international, European and national law enforcement authorities and the necessity of efficient interoperability frameworks to regulate police data and information exchange.

In the context of police cooperation, a crucial parameter that influences the efficiency and effectiveness of the combat of crime is the technical and organisational aspect of transferring systems and database-linkage, as technological interoperability defines and restricts the potential of cooperation approaches and poses the essential fundament to guarantee reliable and secure information sharing.

On the technical level, differences in data format, processing and storage and the lack of appropriate interface specifications hamper the efforts to provide seamless and productive routes for the concatenation of national resources into improved and comprehensive information and analysis systems. To face these challenges, it is inevitable to implement standardised interoperability frameworks that not only specify measures for technical harmonisation but also addresses capabilities and limitations on the legal, organisational and semantic level. The supreme goal is to provide a uniform infrastructural and administrative basis on which appropriate interfaces can be implemented to improve, accelerate and facilitate the processing of exchanged information and data while at the same time minimising the expenses regarding finances and human resources.

In Europe, current efforts to improve police cooperation include the second e-government action plan (2016–2020) in the scope of the Strategy for the European Digital Single Market. The strategy builds on the promotion of a standardised concept model for European public services and offers 47 concrete recommendations for public administrations to help them increase the interoperability of their digital services.

Furthermore, the European Police Office Europol that coordinates the international police cooperation of all 28 EU member states plus associated countries has been investing in improved interoperability on the organisational level by bringing together executives,

experts and decision-makers in the form of Joint Investigation Teams (JIT) and organising Joint Action Days (JAD) to encourage increased direct communication and thereby increasing the success rates of criminal prosecution.

Taken together, these efforts already exhibit impressive successes and demonstrate the potential of international police cooperation to significantly exceed national approaches.

Nevertheless, although established procedures already benefit all EU member states, the organisational and technical alignment of national circumstances in the context of a topic as sensitive as police data exchange will remain challenging and difficult to orchestrate, as the handling and processing of the exchanged information is an issue that has to be addressed vehemently. Not only the accumulation of gigantic amounts of data, but also the regulation of its respective accessibility can become vulnerable targets for abuse, and the situation already fuels justifiable distrust of the government among citizens. As a consequence, to prevent the success of international police cooperation from being tainted by detrimental occurrences harming the people who are supposed to benefit from Europeanisation, data protection and security has to be considered the highest priority on all affected levels.

The digitalisation of Europe harbour great potential for facilitated technical and organisational procedures, and international collaboration, coordination and communication surely promise a valuable asset in preserving the European Union as an Area of Freedom, Security and Justice.

> "With great power comes great responsibility." [1]

[1] [Inv15] - Stan Lee: August 1962.

# List of Figures


3.1 [Eur16c] - Europol's Organisational Structure (eff. 2017). . . . . 31
3.2 [Eur19e] - Eurojust Organigram (eff. 2018). . . . . 36

5.1 [Com16a] - "European Interoperability Timeline". . . . . 60
5.2 [otEU10, p. 14] - "Conceptual model for public services". . . . . 61
5.3 [Eur17c] - "European Search Portal (ESP) and the different databases and their partial interconnection". . . . . 69
5.4 [Cim19] - CIR (Common Identity Repository). . . . . 70

6.1 [Eur14b, p. 3] - "UMF as a layer between systems". . . . . 73
6.2 [Eur14b, p. 4] - "'POLICE' Information Model". . . . . 74
6.3 [Eur17d, p. 72] - Professional Backgrounds of EPE Users. . . . . 84

7.1 [Eur19i] - EU Policy Cycle. . . . . 92

# Acronyms

| | |
|---|---|
| .BK | Bundeskriminalamt - Austrian Federal Criminal Police Office. |
| AFIS | Automated Fingerprint Identification System. |
| AFSJ | Area of Freedom, Security and Justice. |
| AWF | Analytic Working Files. |
| BAKS | Büro-, Automations- und Kommunikationssystem. |
| BDSG | Bundesdatenschutzgesetz. |
| BKA | Bundeskanzleramt. |
| BKA-G | Bundeskriminalamtgesetz. |
| BMDW | Bundesministerium für Digitalisierung und Wirtschaftsstandort. |
| BMI | Bundesministerium für Inneres - Federal Ministry of Internal Affairs. |
| C-SIS | Central Schengen Information System. |
| C4 | Cybercrime Competence Center. |
| CAS | Central Authentification System. |
| CELAD | European Committee to Combat Drugs. |
| CEPOL | Collège Européen de Police - European Police Collage. |
| CFSP | Common Foreign and Security Policy. |
| CIR | Common Identity Repository. |
| COSI | Committee on Operational Cooperation on Internal Security. |
| DNA | Deoxyribonucleic Acid. |
| DPO | Data Protection Officer. |
| EAS | Europol Analysis System. |
| EBDS | European Union Bomb Data System. |

| | |
|---|---|
| EC | European Communities. |
| ECB | European Central Bank. |
| ECDC | European Centre for Disease Prevention and Control. |
| ECJ | European Court of Justice. |
| ECRIS-TCN | European Criminal Records Information System for Third-country Nationals. |
| ECSC | European Coal and Steel Community. |
| ECTC | European Counter Terrorism Centre. |
| EDEN | Europol Dataprotection Experts Networks. |
| EDIAKT | Electronic Data Interchange Akt. |
| EDIDOC | Electronic Data Interchange for Documents. |
| EDPB | European Data Protection Board. |
| EDPS | European Data Protection Supervisor. |
| EDU | Europol Drug Unit. |
| EEC | European Economic Community. |
| EES | Entry/Exit-System. |
| EGC | European General Court. |
| eGIF | e-Government Interoperability Framework. |
| eIDAS | electronic Identification, Authentification and Trust Services. |
| EIF | European Interoperability Framework. |
| EIRA | European Interoperability Reference Architecture. |
| EIS | Europol Information System. |
| EIS | European Interoperability Strategy. |
| EJN | European Judicial Network. |
| EJTN | European Judicial Training Network. |
| EJUP | European Joint Unit on Precursors. |
| EKIS | Elektronisches Kriminalpolizeiliches Informationssystem. |
| ELAK | Elektronischer Akt des Bundes. |
| EMAS | Europol Malware Analysis Systems. |
| EMCDDA | European Monitoring Centre for Drugs and Drug Addiction. |
| EMPACT | European Multidisciplinary Platform against Criminal Threats. |
| ENFAST | European Network of Fugitive Active Search Team. |
| ENFSI | European Network of Forensics Science Institutes. |
| ENISA | European Union Agency for Cybersecurity. |
| ENP | European Network of Policewomen. |

| | |
|---|---|
| EOP | Europol Operation Center. |
| EPA | European Police Association. |
| EPC | European Political Cooperation. |
| EPE | Europol Platform for Experts. |
| EPPO | European Public Prosecutor's Office. |
| ESP | European Search Portal. |
| ETIAS | European Travel Information and Authorisation System. |
| EU | European Union. |
| EU IRU | European Union Internet Referral Unit. |
| eu-LISA | European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice. |
| EUCPN | European Crime Prevention Network. |
| EURATOM | European Atomic Energy Community. |
| EURODAC | European Asylum Dactyloscopy Database. |
| Eurojust | EU Unit for Judicial Cooperation. |
| Europol | European Union Agency for Law Enforcement Cooperation. |
| FIU | Financial Intelligence Unit. |
| FOIA | Freedom of Information Act. |
| Frontex | European Border and Coast Guard Agency. |
| G2B | Government to Business. |
| G2C | Government to Citizens. |
| G2E | Government-to-Employees. |
| G2G | Government to Government. |
| GDP | Gross Domestic Product. |
| GDPR | General Data Protection Regulation. |
| HLEG | High-Level Experts Group. |
| HTTP | Hypertext Transfer Protocol. |
| I-24/7 | Global Communication System 24/7. |
| ICPC | International Criminal Police Commission. |
| ICPO | International Criminal Police Organisation. |
| ICT | Information and Communication Technology. |
| IDABC | Interoperable Delivery of European eGovernment Services to public Administrations, Businesses and Citizens. |
| IDMC | Integrated Data Management Concept. |
| IGC | Intergovernmental Conference. |

| | |
|---|---|
| IKDA | Integrierte Kriminalpolizeiliche Datenanwendung. |
| IKV | Internationale Kriminalistische Vereinigung - International Criminal Union. |
| IOCTA | Internet Organised Crime Threat Assessment. |
| IPA | International Police Association. |
| IPC3 | Intellectual Property Crime Coordinated Coalition. |
| IPEN | Internet Privacy Engineering Network. |
| IPOS | Integriertes Polizeiliches Sicherheitssystem. |
| ISA | Interoperability Solutions for European Public Administrations, Businesses and Citizens. |
| IT | Information Technology. |
| | |
| JAD | Joint Action Days. |
| JHA | Justice and Home Affairs. |
| JIT | Joint Investigation Team. |
| JSON | JavaScript Object Notation. |
| | |
| LFE | Large File Exchange. |
| LKA | Landeskriminalamt. |
| | |
| MASP | Multiannual Strategy Plan. |
| MITC | Missing Trader Intra-Communit. |
| MoU | Memorandum of Understanding. |
| | |
| N-SIS | National Schengen Information System. |
| NIF | National Interoperability Framework. |
| NIFO | National Interoperability Framework Observatory. |
| NIS | Network and Information Systems. |
| NSA | National Security Agency. |
| | |
| OAP | Operational Action Plan. |
| OECD | Organisation for Economic Cooperation and Development. |
| OEEC | Organisation for European Economic Cooperation. |
| OLAF | Office Européen de Lutte Anti-Fraude. |
| | |
| PAD | Protokollieren-Anzeigen-Daten. |
| PAD NG | Protokollieren-Anzeigen-Daten - Next Generation. |

| | |
|---|---|
| PJCC | Police and Judicial Cooperation in Criminal Matters. |
| PKS | Polizeiliche Kriminalstatistik. |
| POLICE | Person, Organisation, Location, Item, Connection, Event. |
| PolKG | Polizeikooperationsgesetz. |
| PWGT | Police Working Group on Terrorism. |
| QUEST | Querying Europol Systems. |
| RAILPOL | European Association of Railway Police Forces. |
| REST | Representational State Transfer. |
| SCAN | Scanning, Analysis and Notification. |
| SEA | Single European Act. |
| SIENA | Secure Information Exchange Network Application. |
| SIRENE | Supplementary Information Request at the National Entry. |
| SIS | Schengen Information System. |
| SLA | Service Level Agreement. |
| SM | Sicherheitsmonitor. |
| SMTP | Simple Mail Transfer Protocol. |
| SOAP | Simple Object Access Protocol. |
| SOCTA | Serious and Organised Crime Threat Assessment. |
| SPOC | Single Point Of Contact. |
| SSL | Secure Sockets Layer. |
| TE-SAT | EU Terrorism Situation and Trend Report. |
| TECS | The Europol Computer System. |
| TEU | Treaty on European Union. |
| TFEU | Treaty on the Functioning of the EU. |
| TREVI | Terrorisme, Radicalisme, Extrémisme et Violence Internationale. |
| UK | United Kingdom. |
| UMF | Universal Message Format. |
| UN | United Nations. |
| UNODC | United Nations Office on Drugs and Crime. |
| USA | United States of America. |
| VAT | Value Added Tax. |

| | |
|---|---|
| VIS | Visa Information System. |
| W3C | World Wide Web Consortium. |
| WfMC | Workflow Management Coalition. |
| XML | eXtensible Markup Language. |
| ZDS | Zentrale Datensammlung. |

# Bibliography


[AE17] Bethany Allen-Ebrahimian. Interpol Is Helping Enforce China's Political Purges. *Foreign Policy*, Apr 2017.

[Age19] European Union Agency. Frontex, Mar 2019. frontex.europa.eu [Online; accessed 25. Mar. 2019].

[And10] Peter Andre. Europaweite Polizeikooperation. *Öffentliche Sicherheit. Das Magazin des Innenministeriums*, 10(3-4):90–93, 2010.

[Apu19] Matt Apuzzo. How Strongmen Turned Interpol Into Their Personal Weapon. *N. Y. Times*, Mar 2019. nytimes.com/2019/03/22/world/europe/interpol-most-wanted-red-notices.html [Online; accessed 16. Apr. 2019].

[Arc09] Christoph Archan. *Die polizeiliche Zusammenarbeit im Rahmen von Schengen: Erfahrungen von Österreich.* Breitenmoser/Gless/Lagodny, 2009.

[Ass19] European Police Association. Who are we ?, Mar 2019. europeanpolice.net/en/who-are-we [Online; accessed 25. Mar. 2019].

[BBPC10] In Warsaw Benedict Brogan Political Correspondent. Blair wants EU to become superpower, Oct 2010. telegraph.co.uk/news/worldnews/europe/poland/1369282/Blair-wants-EU-to-become-superpower.html [Online; accessed 24. Apr. 2019].

[BdI18] Für Bau und Heimat Bundesministerium des Innern. Kriminalprävention. *Bundesministerium des Innern, für Bau und Heimat*, Oct 2018.

[Bor08] Detlef Borchers. Danziger Gespräche: Bessere Polizeikommunikation mit SIENA. *heise online*, Oct 2008. heise.de/newsticker/meldung/Danziger-Gespraeche-Bessere-Polizeikommunikation-mit-SIENA-210307.html [Online; accessed 12. Mar. 2019].

[Bor13] Detlef Borchers. SIS II beginnt am 9. April trotz weiterhin vorhandener Mängel. *heise online*, Mar 2013.

[Bre09] Stephan Breitenmoser. *Die Grundlagen der polizeilichen Zusammenarbeit im Rahmen von Schengen.* University of Basel, 2009.

[Bri19a] Encyclopedia Britannica. Census | Facts, Definition, Methods, & History, Mar 2019. britannica.com/science/census [Online; accessed 26. Mar. 2019].

[Bri19b] Encyclopedia Britannica. Interpol | international organization, Mar 2019. britannica.com/topic/Interpol [Online; accessed 5. Mar. 2019].

[Bun18a] Deutscher Bundestag. Austausch geheim eingestufter Informationen unter europäischen Geheimdiensten, Polizeien und Militärs - BT-Drucksache 18/7034, Nov 2018. dipbt.bundestag.de/extrakt/ba/WP18/709/70978.html [Online; accessed 12. Mar. 2019].

[Bun18b] Bundestministerium Inneres: Bundeskriminalamt. Polizeiliche Kriminalstatistik (PKS) - 2017, Mar 2018. bundeskriminalamt.at/501/files/PKS_17_Broschuere_Web.pdf [Online; accessed 16. Mar. 2019].

[Bun19a] Bundestministerium Inneres. Bundespolizei, Mar 2019. bmi.gv.at/202/start.aspx [Online; accessed 16. Mar. 2019].

[Bun19b] Bundestministerium Inneres: Bundeskriminalamt. Abteilungen im BK, Mar 2019. bundeskriminalamt.at/101/abteilungen.aspx [Online; accessed 25. Mar. 2019].

[Bun19c] Bundestministerium Inneres: Bundeskriminalamt. Das .BK im Überblick, Mar 2019. bundeskriminalamt.at/101/start.aspx [Online; accessed 16. Mar. 2019].

[bUUoL19a] CVCE.EU by UNI.LU (University of Luxembourg). European Political Cooperation (EPC) - Historical events in the European integration process (1945–2014), Apr 2019. cvce.eu/en/collections/unit-content/-/unit/02bb76df-d066-4c08-a58a-d4686a3e68ff/fed975ca-665b-4c89-ac04-0ac7e8919c51 [Online; accessed 15. Apr. 2019].

[bUUoL19b] CVCE.EU by UNI.LU (University of Luxembourg). The Charter of fundamental rights of the European Union - Historical events in the European integration process (1945–2014), Apr 2019. cvce.eu/de/collections/unit-content/-/unit/en/02bb76df-d066-4c08-a58a-d4686a3e68ff/36c0a287-c065-46da-842e-b7f3a9f8c212 [Online; accessed 15. Apr. 2019].

[bUUoL19c] CVCE.EU by UNI.LU (University of Luxembourg). The first pillar of the European Union - Historical events in the European integration process (1945–2014), Apr 2019. cvce.eu/en/recherche/unit-content/-/unit/02bb76df-d066-4c08-a58a-d4686a3e68ff/4ee15c10-5bdf-43b1-9b5f-2553d5a41274 [Online; accessed 15. Apr. 2019].

[bUUoL19d] CVCE.EU by UNI.LU (University of Luxembourg). The political implications of the enlargement of the European Union - Historical events in the European integration process (1945–2014), Apr 2019. cvce.eu/de/collections/unit-content/-/unit/en/02bb76df-d066-4c08-a58a-d4686a3e68ff/7f0adb47-d7ca-4b23-a459-79b68538c4f4 [Online; accessed 15. Apr. 2019].

[bUUoL19e] CVCE.EU by UNI.LU (University of Luxembourg). The second pillar of the European Union: common foreign and security policy - Historical events in the European integration process (1945–2014), Apr 2019. cvce.eu/en/recherche/unit-content/-/unit/02bb76df-d066-4c08-a58a-d4686a3e68ff/280511d5-b97d-4f51-b60d-7496ade168ea [Online; accessed 15. Apr. 2019].

[bUUoL19f] CVCE.EU by UNI.LU (University of Luxembourg). The third pillar of the European Union: justice and home affairs - Historical events in the European integration process (1945–2014), Apr 2019. cvce.eu/en/recherche/unit-content/-/unit/02bb76df-d066-4c08-a58a-d4686a3e68ff/9370a173-d882-4484-974a-f4002c3bd17a [Online; accessed 15. Apr. 2019].

[bUUoL19g] CVCE.EU by UNI.LU (University of Luxembourg). The Treaty of Lisbon - Historical events in the European integration process (1945–2014), Apr 2019. cvce.eu/en/recherche/unit-content/-/unit/02bb76df-d066-4c08-a58a-d4686a3e68ff/d7da2396-d047-4c4e-ae1b-f9edb47e3739 [Online; accessed 15. Apr. 2019].

[Bü18] Bürgerservice des Bundesministeriums für Digitalisierung und Wirtschaftsstandort. Sicherheit, Sep 2018. buergerkarte.at/sicherheit.html [Online; accessed 14. Apr. 2019].

[Cam11] Paolo Campana. Eavesdropping on the Mob: The Functional Diversification of Mafia Activities across Territories. *European Journal of Criminology - EUR J CRIMINOL*, 8:213–228, 05 2011.

[Cen14] IBM Knowledge Center. Universal Message Format (UMF), Oct 2014. ibm.com/support/knowledgecenter/en/SS2HSB_8.1.0/com.ibm.iis.ii.overview.doc/topics/eas_con_umf.html [Online; accessed 8. Apr 2019].

[Cha19] Andrew Charlesworth. A Very Short History of Data Protection, May 2019. cloudview.co/Averyshorthistoryofdataprotection [Online; accessed 12. May 2019].

[Che19] Cloud Privacy Check. A brief history of data protection: How did it all start?, May 2019. cloudprivacycheck.eu/latest-news/article/a-brief-history-of-data-protection-how-did-it-all-start [Online; accessed 12. May 2019].

[Cim19] Catalin Cimpanu. EU votes to create gigantic biometrics database. *ZDNet*, Apr 2019. zdnet.com/article/eu-votes-to-create-gigantic-biometrics-database [Online; accessed 26. Apr. 2019].

[Com87] European Communities. Single European Act, OJ L 169, 29.6.1987, p. 1–28, Jun 1987. data.europa.eu/eli/treaty/sea/sign [Online; accessed 07. Mar. 2019].

[Com90] European Communities. Official Journal of the European Communities, C 262, 17 October 1990, Oct 1990. eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:C:1990:262:TOC [Online; accessed 25. Mar. 2019].

[Com13a] European Commission. Press release - Background on Schengen enlargement, Apr 2013. europa.eu/rapid/press-release_MEMO-07-618_en.htm [Online; accessed 28. Apr. 2019].

[Com13b] European Commission. Press release - Schengen Information System (SIS II) goes live, Apr 2013. europa.eu/rapid/press-release_IP-13-309_en.htm [Online; accessed 28. Apr. 2019].

[Com14] European Commission. European eGovernment Action Plan 2011-2015 - Digital Single Market - European Commission, Oct 2014. ec.europa.eu/digital-single-market/european-egovernment-action-plan-2011-2015 [Online; accessed 25. Mar. 2019].

[Com15] European Commission. A Digital Single Market Strategy for Europe, Jun 2015. eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52015DC0192 [Online; accessed 26. Mar. 2019].

[Com16a] European Commission. About ISA$^2$, Nov 2016. ec.europa.eu/isa2/isa2_en [Online; accessed 12. Mar. 2019].

[Com16b] European Commission. European Public Prosecutor's Office - European Anti-Fraud Office, Feb 2016. ec.europa.eu/anti-fraud/policy/european_public_prosecutor_en [Online; accessed 25. Mar. 2019].

[Com16c] European Commission. Internal Market, Industry, Entrepreneurship and SMEs - The European Single Market, Jul 2016. c.europa.eu/growth/single-market [Online; accessed 16. May 2019].

[Com16d] European Commission. ISA$^2$ - The New European Interoperability Framework, Nov 2016. ec.europa.eu/isa2/eif_en [Online; accessed 12. Mar. 2019].

[Com16e] European Commission. Migration and Home Affairs - SIRENE cooperation, Dec 2016. ec.europa.eu/home-affairs/what-we-do/policies/borders-and-visas/schengen-information-system/sirene-cooperation_en [Online; accessed 12. Apr. 2019].

[Com16f] European Commission. NIFO - ISA$^2$ - European Commission, Nov 2016. ec.europa.eu/isa2/solutions/nifo_en [Online; accessed 12. Apr. 2019].

[Com17a] European Commission. Action Plan to enhance preparedness against chemical, biological, radiological and nuclear security risks, Oct 2017. ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-security/20171018_action_plan_to_enhance_preparedness_against_chemical_biological_radiological_and_nuclear_security_risks_en.pdf [Online; accessed 22. Apr. 2019].

[Com17b] European Commission. Digital Day - Digital Single Market, Feb 2017. ec.europa.eu/digital-single-market/en/digital-day [Online; accessed 13. Mar. 2019].

[Com17c] European Commission. Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), Jan 2017. eur-lex.europa.eu/legal-content/PT/ALL/?uri=celex:52017SC0003 [Online; accessed 16. Apr. 2019].

[Com17d] ISA$^2$ European Commission. The New European Interoperability Framework, Feb 2017. ec.europa.eu/isa2/sites/isa/files/eif_brochure_final.pdf [Online; accessed 27. Feb. 2019].

[Com18a] European Commission. EURODAC (European Asylum Dactyloscopy Database) - Knowledge for policy European Commission, Oct 2018. ec.europa.eu/knowledge4policy/dataset/ds00008_en [Online; accessed 24. Mar. 2019].

[Com18b] European Commission. Press release - State of the Union 2018: Commission proposes new rules to get terrorist content off the web, Sep 2018. europa.eu/rapid/press-release_IP-18-5561_en.htm [Online; accessed 28. Apr. 2019].

[Com18c] European Commission. What information must be given to individuals whose data is collected?, Jan 2018. web.archive.org/web/20180523102419/https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/principles-gdpr/what-information-must-be-given-individuals-whose-data-collected_en [Online; accessed 12. Mar. 2019].

[Com19a] European Commission. About INSPIRE, Apr 2019. inspire.ec.europa.eu/about-inspire/563 [Online; accessed 17. Apr. 2019].

[Com19b] European Commission. European Anti-Fraud Office, Mar 2019. ec.europa.eu/anti-fraud/home_en [Online; accessed 25. Mar. 2019].

[Con18] World Wide Web Consortium. About W3C, Dec 2018. w3.org/Consortium [Online; accessed 22. Mar. 2019].

[Cou08] European Council. Council Decision 2009/426/JHA of 16 December 2008 on the strengthening of Eurojust and amending Decision 2002/187/JHA setting up Eurojust with a view to reinforcing the fight against serious crime, Dec 2008. data.europa.eu/eli/dec/2009/426/oj [Online; accessed 30. Mar. 2019].

[Cou09] Council of European Union. Council Decision of 6 April 2009 establishing the European Police Office (Europol) - (2009/371/JHA), 2009. eur-lex.europa.eu/eli/dec/2009/371/oj.

[Cou15] Council of European Union. Council regulation (EU) no 2015/2240, Nov 2015. data.europa.eu/eli/dec/2015/2240/oj [Online; accessed 12. Mar. 2019].

[Cou16] Council of European Union. Enhancing counter terrorism capabilities at EU level: European Counter Terrorism Centre (ECTC) at Europol and counter terrorism related information sharing. no. 14244/15, Nov 2016. statewatch.org/news/2015/nov/eu-council-europol-ECTC-14244-15.pdf [Online; accessed 12. Mar. 2019].

[Cou17] Council Regulation. Council Regulation (EU) 2017/1939 of 12 October 2017 implementing enhanced cooperation on the establishment of the European Public Prosecutor's Office ('the EPPO'), Oct 2017. eur-lex.europa.eu/eli/reg/2017/1939/oj [Online; accessed 24. Apr. 2019].

[dB19a] Rechtsinformationssystems des Bundes. RIS - Bundesgesetz über die Einrichtung und Organisation des Bundeskriminalamtes (Bundeskriminalamt-Gesetz – BKA-G), Mar 2019. ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20001745 [Online; accessed 15. Mar. 2019].

[dB19b] Rechtsinformationssystems des Bundes. RIS - Bundesministeriengesetz 1986, May 2019. ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10000873 [Online; accessed 11. May 2019].

[dB19c] Rechtsinformationssystems des Bundes. RIS - EU – Polizeikooperationsgesetz, Mar 2019. ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20006630 [Online; accessed 15. Mar. 2019].

[dB19d] Rechtsinformationssystems des Bundes. RIS - Übereinkommen auf Grund von Art. K.3 des Vertrags über die Europäische Union

über die Errichtung eines Europäischen Polizeiamts (Europol-Übereinkommen) samt Anhang und Erklärungen, Mar 2019. ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen& Gesetzesnummer=10006071 [Online; accessed 17. Mar. 2019].

[dB20] Rechtsinformationssystems des Bundes. RIS - Bundesgesetz zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten (Datenschutzgesetz – DSG), Mar 2020. ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=bundesnormen&Gesetzes nummer=10001597 [Online; accessed 29. Mar. 2020].

[Deg03] Kerstin Degenhardt. EUROPOL und Strafprozess. *Die Europäisierung des Ermittlungsverfahrens. Frankfurt a. M*, 2003.

[Dic19] Cambridge English Dictionary. the NSA, Apr 2019. dictionary.cambridge.org/dictionary/english/nsa [Online; accessed 24. Apr. 2019].

[Die11] Deutscher Bundestag: Wissenschaftliche Dienste. Aktueller Begriff - Europa: Das ordentliche Gesetzgebungsverfahren, 2011. web.archive.org/web/20110516153250/http://www.bundestag.de/dokumente/analysen/2011/ordentliches_Gesetzgebungsverfahren.pdf [Online; accessed 12. Mar. 2019].

[Dud] Duden. | Interoperabilität | Rechtschreibung, Bedeutung, Definition. duden.de/node/688795/revisions/1780313/view [Online; accessed 12. Mar. 2019].

[Edi09] History.com Editors. Marshall Plan. *HISTORY*, 2009. history.com/topics/world-war-ii/marshall-plan-1 [Online; accessed 15. May 2019].

[EL85] EUR-Lex. Summaries of EU Legislation - Schengen (Agreement and Convention), Jun 1985. eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM%3Aschengen_agreement [Online; accessed 30. Mar. 2019].

[EL09] EUR-Lex. Europol: Europäisches Polizeiamt (bis 31.12.2009), Sep 2009. eur-lex.europa.eu/legal-content/DE/TXT/?uri=LEGISSUM:l14005b [Online; accessed 13. Mar. 2019].

[EL14] EUR-Lex. From the Schengen Information System (SIS 1+) to the second generation Schengen Information System (SIS II), Oct 2014. eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM:jl0010 [Online; accessed 22. Apr. 2019].

[EL19a] EUR-Lex. Europol Drugs Unit, Mar 2019. eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM:l14005a [Online; accessed 5. Mar. 2019].

[EL19b] EUR-Lex. Glossary of summaries - Accession Criteria (Copenhagen Criteria), Apr 2019. eur-lex.europa.eu/summary/glossary/accession_criteria_copenhague.html [Online; accessed 15. Apr. 2019].

[Enc18] New World Encyclopedia. Interoperability, Mar 2018. newworldencyclopedia.org/entry/Interoperability [Online; accessed 15. Mar. 2019].

[ENP19] ENP. About | ENP (European Network of Policewomen), May 2019. enp.eu/about [Online; accessed 21. May 2019].

[ePr18] ePrivacy. What does the ePrivacy Regulation mean for the online industry?, Feb 2018. eprivacy.eu/en/about-us/news-press/news-detail/article/what-does-the-eprivacy-regulation-mean-for-the-online-industry [Online; accessed 11. May 2019].

[ES17] E-Spin. Definition and Type of E-Government. *E-SPIN Group*, Dec 2017. e-spincorp.com/definition-and-type-of-e-government [Online; accessed 21. Mar. 2019].

[EU 15] EU Intelligence Analysis Centre (EU INTCEN). INTCEN Fact Sheet, Feb 2015. web.archive.org/web/20160214025522/http://eeas.europa.eu/factsheets/docs/20150206_factsheet_eu_intcen_en.pdf [Online; accessed 24. Mar. 2019].

[EUC19] EUCPN. European Crime Prevention Network - About EUCPN, Apr 2019. eucpn.org/about/network [Online; accessed 9. Apr. 2019].

[Eur] Europol. Europol Information Management Booklet, File no: 2510-271. euro-police.noblogs.org/gallery/3874/Europol%20Products%20and%20Services-Booklet.pdf [Online; accessed 16. Mar. 2019].

[Eur99] Europol. 1 July 1999 - Europol takes up its full activities!, Jul 1999. web.archive.org/web/20091015053551/http://www.europol.europa.eu/index.asp?page=news&news=pr990701.htm [Online; accessed 7. Mar. 2019].

[Eur01a] European Communities. Treaty of Nice amending the Treaty on European Union, the Treaties establishing the European Communities and certa in related acts - Declarations Adopted By The Conference - Declaration on the future of the Union, Mar 2001. data.europa.eu/eli/treaty/nice/fna_1/dcl_23/sign [Online; accessed 15. Apr. 2019].

[Eur01b] Europol. Press release - Europol and Interpol sign a Co-operation Agreement, Nov 2001. web.archive.org/web/20091015074455/http://www.europol.europa.eu/index.asp?page=news&news=pr011105.htm [Online; accessed 29. Mar. 2019].

[Eur01c] Europol. Press release - USA and Europol join forces in fighting terrorism!, Dec 2001. web.archive.org/web/20091015085148/http://www.europol.europa.eu/index.asp?page=news&news=pr011211.htm [Online; accessed 29. Apr. 2019].

[Eur03] European Parliament and of the Council. 2004/55/EC: Decision of the European Parliament and of the Council of 22 December 2003 appointing the independent supervisory body provided for in Article 286 of the EC Treaty (European Data Protection Supervisor), Dec 2003. eur-lex.europa.eu/eli/dec/2004/55(1)/oj [Online; accessed 24. Apr. 2019].

[Eur09] Europol. Europol Review 2009, 2009. europol.europa.eu/activities-services/main-reports/europol-review-2009 [Online; accessed 26. Apr. 2019].

[Eur10] European Commission. The European eGovernment Action Plan 2011-2015 Harnessing ICT to promote smart, sustainable & innovative Government, Dec 2010. eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0743:FIN:EN:PDF [Online; accessed 9. Mar. 2019].

[Eur12] Europol. SIENA, Secure Information Exchange Network Application. *Publications Office of the European Union*, Mar 2012. publications.europa.eu/en/publication-detail/-/publication/bf5426ff-929f-4f0b-ba2a-1d2793dc3030 [Online; accessed 12. Mar. 2019].

[Eur13] Europol. Europol Information System (EIS) Leaflet, 2013. europol.europa.eu/publications-documents/europol-information-system-eis-leaflet [Online; accessed 15. Mar. 2019].

[Eur14a] European Parliament and of the Council. Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, Jul 2014. data.europa.eu/eli/reg/2014/910/oj [Online; accessed 9. Mar. 2019].

[Eur14b] Europol. Universal Message Format : faster, cheaper, better. *Publications Office of the European Union*, Apr 2014. publications.europa.eu/s/llVy.

[Eur16a] European Commission. EU eGovernment Action Plan 2016-2020, Accelerating the digital transformation of government, Apr 2016. eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52016DC0179 [Online; accessed 9. Mar. 2019].

[Eur16b] European Union. Court of Justice of the European Union, Jun 2016. europa.eu/european-union/about-eu/institutions-bodies/court-justice_en [Online; accessed 23. Mar. 2019].

[Eur16c] Europol. About Europol, Sep 2016. europol.europa.eu/about-europol [Online; accessed 10. Sep. 2016].

[Eur16d] Europol. Europol Review 2015, 2016. europol.europa.eu/activities-services/main-reports/europol-review-2015 [Online; accessed 28. Apr. 2019].

[Eur17a] European Commission. European Public Prosecutor's Office, Jun 2017. ec.europa.eu/info/law/cross-border-cases/judicial-cooperation/networks-and-bodies-supporting-judicial-cooperation/european-public-prosecutors-office_en [Online; accessed 12. Mar. 2019].

[Eur17b] European Commission, Directorate-General for Informatics. Communication From The Commission To The European Parliament, The Council, The European Economic And Social Committee And The Committee Of The Regions - European Interoperability Framework – Implementation Strategy, Mar 2017. eur-lex.europa.eu/legal-content/EN/ALL/?uri=COM:2017:134:FIN [Online; accessed 14. Apr. 2019].

[Eur17c] European Commission, Directorate-General for Migration and Home Affairs. Proposal for a Regulation Of the European Parliament and of the Council on establishing a framework for interoperability between EU information systems (police and judicial cooperation, asylum and migration), Dec 2017. eur-lex.europa.eu/legal-content/EN/ALL/?uri=COM:2017:0794:FIN [Online; accessed 14. Apr. 2019].

[Eur17d] Europol. Europol Review 2016 - 2017, 2017. europol.europa.eu/activities-services/main-reports/europol-review-2016-2017 [Online; accessed 25. Mar. 2019].

[Eur18] Europol. EU Terrorism Situation & Trend Report (Te-Sat), 2018. europol.europa.eu/activities-services/main-reports/eu-terrorism-situation-and-trend-report [Online; accessed 15. Mar. 2019].

[Eur19a] Eurojust. College of Eurojust, Apr 2019. eurojust.europa.eu/about/structure/college/Pages/college.aspx [Online; accessed 16. Apr. 2019].

[Eur19b] Eurojust. History of Eurojust, Mar 2019. eurojust.europa.eu/about/background/Pages/history.aspx [Online; accessed 12. Mar. 2019].

[Eur19c] Eurojust. Independent Joint Supervisory Body, Mar 2019. eurojust.europa.eu/jsb.htm Online; accessed 5. Mar. 2019].

[Eur19d] Eurojust. Mission and Tasks, Mar 2019. eurojust.europa.eu/about/background/Pages/mission-tasks.aspx [Online; accessed 12. Mar. 2019].

[Eur19e] Eurojust. Organisational structure, Mar 2019. eurojust.europa.eu/about/structure/Pages/organisational-structure.aspx [Online; accessed 12. Mar. 2019].

[Eur19f] European Judicial Network. About EJN, Mar 2019. ejn-crimjust.europa.eu/ejn/EJN_DynamicPage/EN/1 [Online; accessed 24. Mar. 2019].

[Eur19g] Europol. Data Protection & Transparency, Apr 2019. europol.europa.eu/about-europol/data-protection-transparency [Online; accessed 28. Apr. 2019].

[Eur19h] Europol. EMPACT Joint Action Days generate big results in 2018, Apr 2019. europol.europa.eu/newsroom/news/empact-joint-action-days-generate-big-results-in-2018 [Online; accessed 8. Apr. 2019].

[Eur19i] Europol. EU Policy Cycle - EMPACT, Apr 2019. europol.europa.eu/empact [Online; accessed 8. Apr. 2019].

[Eur19j] Europol. European Counter Terrorism Centre - ECTC, Apr 2019. europol.europa.eu/about-europol/european-counter-terrorism-centre-ectc [Online; accessed 8. Apr. 2019].

[Eur19k] Europol. Europol Information System (EIS), Mar 2019. europol.europa.eu/activities-services/services-support/information-exchange/europol-information-system [Online; accessed 28. Mar. 2019].

[Eur19l] Europol. Europol's 20 most noteworthy operations, Apr 2019. europol.europa.eu/about-europol/europols-20-most-noteworthy-operations [Online; accessed 23. Apr. 2019].

[Eur19m] Europol. Intellectual Property Crime Coordinated Coalition - IPC3, Mar 2019. europol.europa.eu/about-europol/intellectual-property-crime-coordinated-coalition-ipc3 [Online; accessed 25. Mar. 2019].

[Eur19n] Europol. JITs Practical Guide, Apr 2019. europol.europa.eu/publications-documents/jits-practical-guide [Online; accessed 8. Apr. 2019].

[Eur19o] Europol. Joint Action Days (JADs), Apr 2019. europol.europa.eu/operations/joint-action-days-jads [Online; accessed 8. Apr. 2019].

[Eur19p] Europol. Joint Investigation Teams - JITs, Apr 2019. europol.europa.eu/activities-services/joint-investigation-teams [Online; accessed 8. Apr. 2019].

[Eur19q] Europol. Operational Centre, Mar 2019. europol.europa.eu/activities-services/services-support/operational-coordination/operational-centre [Online; accessed 15. Mar. 2019].

[Eur19r] Europol. Statistics & Data, Mar 2019. europol.europa.eu/about-europol/statistics-data [Online; accessed 7. Mar. 2019].

[Eur19s] Europol. Strategic Analysis, Apr 2019. europol.europa.eu/activities-services/services-support/strategic-analysis [Online; accessed 16. Mar. 2019].

[Feh01] János Fehérváry. *Europäisierung der Polizeiarbeit Ein Resultat polizeilicher Kooperation*. J./W. Stangl (Hrsg.), 2001.

[Feh09] János Fehérváry. Funktionale und geografische Strukturen der Zusammenarbeit. Internationale polizeiliche Zusammenarbeit in Europa. *Deutsches Polizeiblatt*, 5, 2009.

[fI17] Bundesministerium für Inneres. Die Sicherheitsdoktrin des BMI für Österreich 2017-2020, Mar 2017. bmi.gv.at/bmi_documents/1977.pdf [Online; accessed 11. Mar 2019].

[fI18a] Bundesministerium für Inneres. Das BMI-Engagement in der Europäischen Union, 2018. bmi.gv.at/509/Agenturen/europol.aspx [Online; accessed 8. Mar. 2019].

[fI18b] Bundesministerium für Inneres. Internationale Zusammenarbeit - 38 Spezialeinheiten schließen sich mit Europol zusammen - Artikel Nr: 16318, Oct 2018. bmi.gv.at/news.aspx?id=4A4E504D7841305839596F3D [Online; accessed 15. Apr. 2019].

[Fou15] Open Dialogue Foundation. The report: The Interpol system is in need of reform, Feb 2015. en.odfoundation.eu/a/5947,the-report-the-interpol-system-is-in-need-of-reform [Online; accessed 16. Apr. 2019].

[GKM+91] Anne Geraci, Freny Katki, Louise McMonegal, Bennett Meyer, John Lane, Paul Wilson, Jane Radatz, Mary Yee, Hugh Porteous, and Fredrick Springsteel. *IEEE standard computer dictionary: Compilation of IEEE standard computer glossaries*. IEEE Press, 1991.

[Gre12] Graham Greenleaf. Global data privacy laws: 89 countries, and accelerating. *Privacy Laws & Business International Report*, (115), 2012.

[Gre17] Graham Greenleaf. Global data privacy laws 2017: 120 national data privacy laws, including Indonesia and Turkey. *Including Indonesia and Turkey (January 30, 2017)*, 145:10–13, 2017.

[Gro19] The Egmont Group. About, Mar 2019. egmontgroup.org/content/about [Online; accessed 25. Mar. 2019].

[Gø10] John Gøtze. European Interoperability Framework 2.0, Dec 2010. gotze.eu/2010/12/19/european-interoperability-framework-2-0 [Online; accessed 9. Mar. 2019].

[Heu07] Kristina Heußner. *Informationssysteme im europäischen Verwaltungsverbund*, volume 17. Mohr Siebeck, 2007.

[HJ07] Chun Hai and Ibrahim Jeong. *Fundamental of development administration*. Scholar, 2007.

[HM19] Nicole Hery-Moßmann. XML - was ist das? Einfach erklärt, Apr 2019. praxistipps.chip.de/xml-was-ist-das-einfach-erklaert_47836 [Online; accessed 8. Apr. 2019].

[Hol06] Andreas Holzer. *Die internationale polizeiliche Zusammenarbeit zur Bekämpfung des Terrorismus und der organisierten Kriminalität innerhalb der Europäischen Union*. Universität Wien, 2006.

[Hum96] Hummer/Obwexer. *Österreich in der Europäischen Union. Die Schengener Übereinkommen und die Zusammenarbeit in den Bereichen Justiz und Inneres, Band III*. Verlag Österreich, Wien, 1996.

[Hüt14] M. Große Hüttmann. Multi-Level-Governance | bpb. *bpb.de*, Jan 2014. bpb.de/nachschlagen/lexika/das-europalexikon/177146/multi-level-governance [Online; accessed 24. Mar. 2019].

[IDA16] IDABC. European Interoperability Framework for pan-European eGovernment services, Nov 2016. ec.europa.eu/idabc/en/document/2319/5938.html [Online; accessed 14. Mar. 2019].

[Int16] Interpol. INTERPOL communication system I-24/7, Sep 2016. interpol.int/en/News-and-media/Publications2/Fact-sheets/Connecting-police-I-24-7 [Online; accessed 10. Sep. 2016].

[Int19a] Interoperability Solutions for European Public Administrations. About the European Interoperability Reference Architecture, Apr 2019. joinup.ec.europa.eu/solution/eira/release/v300 [Online; accessed 17. Apr. 2019].

[Int19b] Interpol. Capacity building projects, Mar 2019. interpol.int/How-we-work/Capacity-building/Capacity-building-projects [Online; accessed 8. Mar. 2019].

[Int19c] Interpol. Global Policing Goals, Mar 2019. interpol.int/Who-we-are/Strategy/Global-Policing-Goals [Online; accessed 5. Mar. 2019].

[Int19d] Interpol. INTERPOL member countries, Apr 2019. interpol.int/Who-we-are/Member-countries [Online; accessed 25. Apr. 2019].

[Int19e] Interpol. INTERPOL's Global Learning Centre, Mar 2019. interpol.int/How-we-work/Capacity-building/INTERPOL-s-Global-Learning-Centre [Online; accessed 8. Mar. 2019].

[Int19f] Interpol. Membership of INTERPOL, Mar 2019. interpol.int/en/Who-we-are/Legal-framework/Membership-of-INTERPOL [Online; accessed 12. Mar. 2019].

[Int19g] Interpol. Name and logo, Apr 2019. interpol.int/en/Who-we-are/Legal-framework/Name-and-logo [Online; accessed 25. Apr. 2019].

[Int19h] Interpol. NCB and police training, Mar 2019. interpol.int/How-we-work/Capacity-building/NCB-and-police-training [Online; accessed 8. Mar. 2019].

[Int19i] Interpol. Neutrality (Article 3 of the Constitution), Mar 2019. interpol.int/About-INTERPOL/Legal-materials/Neutrality-Article-3-of-the-Constitution [Online; accessed 5. Mar. 2019].

[Int19j] Interpol. Our 17 databases, Mar 2019. interpol.int/How-we-work/Databases/Our-17-databases [Online; accessed 8. Mar. 2019].

[Int19k] Interpol. Our Funding, Apr 2019. interpol.int/en/Who-we-are/Our-funding [Online; accessed 25. Apr. 2019].

[Int19l] Interpol. What is INTERPOL?, Mar 2019. interpol.int/Who-we-are/What-is-INTERPOL [Online; accessed 12. Mar. 2019].

[Inv15] Quote Investigator. With Great Power Comes Great Responsibility, Jun 2015. quoteinvestigator.com/2015/07/23/great-power [Online; accessed 15. May 2019].

[IP12] IT-Planungsrat. Kooperationsgruppe Europäische Interoperabilisierung, May 2012.

[IPA19] IPA. International Police Association, Mar 2019. ipa-international.org [Online; accessed 14. Mar. 2019].

[JKK06] Markus Jachtenfuchs and Beate Kohler-Koch. Europäische Integration - Wiesbaden: VS Verlag für Sozialwissenschaften, 2006.

[Jon14] A. Jonas. Intergouvernementale Zusammenarbeit | bpb. *bpb.de*, Jan 2014. bpb.de/nachschlagen/lexika/das-europalexikon/177060/intergouvernementale-zusammenarbeit [Online; accessed 24. Mar. 2019].

[Käm01] Gregor Kämper. *Polizeiliche Zusammenarbeit in der Europäischen Union: Entwicklung, Rechtsformen, grundgesetzliche Zulässigkeit.* Lang, 2001.

[Kil04] Kimmo Kiljunen. *The European Constitution in the making.* CEPS, 2004.

[Kne01] Wilhelm Knelangen. *Das Politikfeld innere Sicherheit im Integrationsprozess: Die Entstehung einer europäischen Polititk der inneren Sicherheit*, volume 4. Springer-Verlag, 2001.

[KP08] Daniela Kietz and Roderick Parkes. Justiz-und innenpolitik nach dem lissabonner vertrag. *Diskussionspapier der Forschungsgruppe*, 1, 2008.

[Kri18] Kristiina Milt. Polizeiliche Zusammenarbeit | Kurzdarstellungen zur Europäischen Union | Europäisches Parlament, Oct 2018. europarl.europa.eu/factsheets/de/sheet/156/polizeiliche-zusammenarbeit [Online; accessed 12. Mar. 2019].

[Krö04] Nicoletta Kröger. *Europol: europäisches Polizeiamt und Individualschutz; Vereinbarkeit mit Grundgesetz und Europäischer Menschenrechtskonvention?* Peter Lang, Frankfurt am Main, 2004.

[KV02] Martin Kraus-Vonjahr. Der Aufbau eines Raums der Freiheit, der Sicherheit und des Rechts in Europa. *Frankfurt aM*, 2002.

[Lit10] Romana Litzka. Polizeiliche Kooperation in der Europäischen Union. Master's thesis, Universität Wien, 2010.

[LS14] Ana Lisboa and Delfina Soares. E-government Interoperability Frameworks: A Worldwide Inventory. *Procedia Technology*, 16:638 – 648, 2014.

[MA16] European Commission Migration and Home Affairs. Visa Information System (VIS), Dec 2016. ec.europa.eu/home-affairs/what-we-do/policies/borders-and-visas/visa-information-system_en [Online; accessed 24. Mar. 2019].

[Mad00] Shirin Madon. The Internet and socio-economic development: exploring the interaction. *Information Technology & People*, Jun 2000.

[MC16a] Migration and Home Affairs European Commission. Schengen Information System, Dec 2016. ec.europa.eu/home-affairs/what-we-do/policies/borders-and-visas/schengen-information-system_en [Online; accessed 15. Apr. 2019].

[MC16b] Migration and Home Affairs European Commission. Second generation Schengen Information System (SIS II), Dec 2016. ec.europa.eu/home-affairs/content/second-generation-schengen-information-system-sis-ii_en [Online; accessed 15. Apr. 2019].

[Mil03] Tile Milke. *Europol und Eurojust: zwei Institutionen zur internationalen Verbrechensbekämpfung und ihre justitielle Kontrolle*, volume 11. Vandenhoeck & Ruprecht, 2003.

[Mil19] Kristiina Milt. Personal data protection | Fact Sheets on the European Union | European Parliament, May 2019. europarl.europa.eu/factsheets/en/sheet/157/personal-data-protection [Online; accessed 16. May 2019].

[Mon10] Matthias Monroy. Europol – Sammelwut ohne Kontrolle, Jan 2010. europolice.noblogs.org/2010/01/europol-sammelwut-ohne-kontrolle [Online; accessed 24. Mar. 2019].

[Mon16] Matthias Monroy. Kein Grund zum Feiern: Start des neuen europäischen Geheimdienstzentrums, Jul 2016. netzpolitik.org/2016/kein-grund-zum-feiern-start-des-neuen-europaeischen-geheimdienstzentrums [Online; accessed 12. Mar. 2019].

[Mon18] Matthias Monroy. Europol vereinfacht Rasterfahndung in polizeilichen Datenbanken, Jun 2018. netzpolitik.org/2018/europol-vereinfacht-rasterfahndung-in-polizeilichen-datenbanken [Online; accessed 7. Apr 2019].

[Mon19] Matthias Monroy. EU merges biometric data pots: Now the query tsunami is coming, Feb 2019. digit.site36.net/2019/02/06/eu-merges-biometric-data-pots-now-the-query-tsunami-is-coming/ [Online; accessed 26. Apr. 2019].

[Mut10] Stefanie Mutschler. *Der Prümer Vertrag: neue Wege der Kriminalitätsbekämpfung auf europäischer Ebene.* Schriften zum Recht der inneren Sicherheit. Boorberg, 2010.

[MV16] Landespolizei Mecklenburg-Vorpommern. Danziger Gespräche, Dec 2016. web.archive.org/web/20161209061638/https://www.polizei.mvnet.de/Presse/Danziger-Gespr%C3%A4che/ [Online; accessed 22. Mar. 2019].

[Nat15] United Nations. Universal Declaration of Human Rights, Oct 2015. un.org/en/universal-declaration-human-rights [Online; accessed 30. Mar. 2019].

[Net19] European Judicial Training Network. About us - EJTN Website, Mar 2019. ejtn.eu/About-us [Online; accessed 25. Mar. 2019].

[Nos04] Harald Noschiel. IPOS - Erfolgreicher Testbetrieb. *Öffentliche Sicherheit. Das Magazin des Innenministeriums*, 4(7-8), 2004.

[Obe98] Rainer Oberleitner. *Schengen und Europol: Kriminalitätsbekämpfung in einen Europa der inneren Sicherheit.* Manz., 1998.

[oE19] Council of Europe. Chart of signatures and Ratifications of Treaty 108 - Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data - Status as of 22/03/2019, Mar 2019. coe.int/en/web/conventions/full-list/-/conventions/treaty/108 [Online; accessed 22. Mar. 2019].

[OEC13] OECD. Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, 2013. oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm [Online; accessed 17. Mar. 2019].

[OEC19a] OECD. History, May 2019. oecd.org/about/history [Online; accessed 12. May 2019].

[OEC19b] OECD. OECD Privacy Guidelines, May 2019. oecd.org/internet/ieconomy/privacy-guidelines.htm [Online; accessed 12. May 2019].

[OEC19c] OECD. Our global reach, May 2019. oecd.org/about/members-and-partners/ [Online; accessed 12. May 2019].

[ÖD19] Österreichische Datenschutzbehörde. Das Schengener Informationssystem der 2. Generation, Apr 2019. dsb.gv.at/-/das-schengener-informationssystem-der-2-generation [Online; accessed 22. Apr. 2019].

[Öst19a] Digitales Österreich. Elektronischer Akt (ELAK), Apr 2019. digitales.oesterreich.gv.at/elektronischer-akt-elak- [Online; accessed 22. Apr. 2019].

[Öst19b] Digitales Österreich. Kommunikationsarchitektur, Apr 2019. digitales.oesterreich.gv.at/kommunikationsarchitektur [Online; accessed 11. Apr. 2019].

[otEU02a] Council of the European Union. Council decision of 28 February 2002 setting up Eurojust with a view to reinforcing the fight against serious crime (2002/187/JHA), Feb 2002. data.europa.eu/eli/dec/2002/187/2009-06-04 [Online; accessed 17. Mar. 2019].

[otEU02b] Council of the European Union. Council Framework Decision of 13 June 2002 on joint investigation teams, Jun 2002. eur-lex.europa.eu/eli/dec_framw/2002/465/oj [Online; accessed 9. Mar. 2019].

[otEU05] Council of the European Union. Prüm Convention, May 2005. ec.europa.eu/anti-fraud/sites/antifraud/files/docs/body/prumtr.pdf [Online; accessed 17. Mar. 2019].

[otEU10] Council of the European Union. Annex 2 to the Communication from the Commission to the European Parliament, the Council, the

European Economic and Social Committee and the Committee of Regions 'Towards interoperability for European public services', Aug 2010. ec.europa.eu/transparency/regdoc/rep/1/2010/EN/1-2010-744-EN-F1-1-ANNEX-2.Pdf [Online; accessed 17. Mar. 2019].

[otEU14] Council of the European Union. Der EU-Politikzyklus zur Bekämpfung der organisierten und schweren internationalen Kriminalität (2014-2017), 2014. consilium.europa.eu/media/30214/qc0114638den.pdf [Online; accessed 8. Apr. 2019].

[otEU16] Council of the European Union. Universal Message Format (UMF) 3 - Proposal for the 5th IMS action list, Mar 2016. data.consilium.europa.eu/doc/document/ST-6882-2016-INIT/en/pdf [Online; accessed 30. Mar. 2019].

[otEU18a] Council of the European Union. The EU policy cycle to tackle organised and serious international crime (2018-2021), 2018. consilium.europa.eu/media/37340/20185274_qc0418775enn_pdf.pdf [Online; accessed 8. Apr. 2019].

[otEU18b] Official Journal of the European Union. Statement of revenue and expenditure of the European Police Office for the financial year 2018, Jun 2018. europol.europa.eu/sites/default/files/documents/c108_142.pdf [Online; accessed 10. Mar. 2019].

[otEU19a] Council of the European Union. The EU fight against organised crime, Mar 2019. consilium.europa.eu/en/policies/eu-fight-against-organised-crime-2018-2021 [Online; accessed 9. Mar. 2019].

[otEU19b] Council of the European Union. The ordinary legislative procedure, Apr 2019. consilium.europa.eu/en/council-eu/decision-making/ordinary-legislative-procedure [Online; accessed 17. Apr. 2019].

[otEU20] Council of the European Union. Justice and Home Affairs Council configuration (JHA), Mar 2020. consilium.europa.eu/en/council-eu/configurations/jha/ [Online; accessed 30. Mar. 2019].

[Pal02] Jacob Palme. The Swedish Personal Information Act, Jun 2002. people.dsv.su.se/ jpalme/society/eu-data-directive-freedom.html [Online; accessed 15. Mar. 2019].

[Par01] European Parliament. European Parliament resolution on the Treaty of Nice and the future of the European Union, May 2001. eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52001IP0168 [Online; accessed 15. Apr. 2019].

[Par02] European Parliament. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), Jul 2002. eur-lex.europa.eu/eli/dir/2002/58/oj [Online; accessed 26. Mar. 2019].

[Par19a] European Parliament. Der Vertrag von Nizza und der Konvent über die Zukunft Europas | Kurzdarstellungen zur Europäischen Union , Apr 2019. europarl.europa.eu/factsheets/de/sheet/4/der-vertrag-von-nizza-und-der-konvent-uber-die-zukunft-europas [Online; accessed 15. Apr. 2019].

[Par19b] European Parliament. Digital Agenda for Europe | Fact Sheets on the European Union, Mar 2019. europarl.europa.eu/factsheets/en/sheet/64/digital-agenda-for-europe [Online; accessed 13. Mar. 2019].

[Par19c] European Parliament. The internal market | Fact Sheets on the European Union, Mar 2019. europarl.europa.eu/factsheets/en/section/189/the-internal-market [Online; accessed 25. Mar. 2019].

[Pia16] Pierre Piazza. Alphonse Bertillon and the Identification of Persons (1880-1914). *Criminocorpus*, Aug 2016.

[PotC95] European Parliament and of the Council. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Oct 1995. eur-lex.europa.eu/eli/dir/1995/46/oj [Online; accessed 30. Mar. 2019].

[PotC02] European Parliament and of the Council. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), Jul 2002. eur-lex.europa.eu/eli/dir/2002/58/oj [Online; accessed 30. Mar. 2019].

[PotC09] European Parliament and of the Council. Decision No 922/2009/EC of the European Parliament and of the Council of 16 September 2009 on interoperability solutions for European public administrations (ISA), Sep 2009. data.europa.eu/eli/dec/2009/922/oj [Online; accessed 07. Mar. 2019].

[PotC15] European Parliament and of the Council. Regulation (EU) 2015/2219 of the European Parliament and of the Council of 25 November 2015 on the European Union Agency for Law Enforcement Training (CEPOL) and replacing and repealing Council Decision 2005/681/JHA, Nov 2015. eur-lex.europa.eu/eli/reg/2015/2219/oj [Online; accessed 30. Mar. 2019].

[PotC16a] European Parliament and of the Council. Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, Apr 2016. data.europa.eu/eli/dir/2016/680/oj [Online; accessed 29. Mar. 2020].

[PotC16b] European Parliament and of the Council. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Apr 2016. data.europa.eu/eli/reg/2016/679/oj [Online; accessed 13. Mar. 2019].

[PotC16c] European Parliament and of the Council. Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA, May 2016. data.europa.eu/eli/reg/2016/794/oj [Online; accessed 07. Mar. 2019].

[PotC18] European Parliament and of the Council. Regulation (EU) 2018/1727 of the European Parliament and of the Council of 14 November 2018 on the European Union Agency for Criminal Justice Cooperation (Eurojust), and replacing and repealing Council Decision 2002/187/JHA, Nov 2018. eur-lex.europa.eu/eli/reg/2018/1727/oj [Online; accessed 30. Mar. 2019].

[PS07] Shailendra C Jain Palvia and Sushil S Sharma. E-government and e-governance: definitions/domain framework and status around the world. In *International Conference on E-governance*, number 5, pages 1–12, 2007.

[RAI19] RAILPOL. About RAILPOL - European Association of Railway Police Forces, Mar 2019. railpol.eu/site/about-railpol [Online; accessed 21. Mar. 2019].

[Rat08] Max-Peter Ratzel. Das Europäische Polizeiamt. Europol (Teil 1). *.SIAK-Journal – Zeitschrift für Polizeiwissenschaft und polizeiliche Praxis*, 1(1):27–37, 2008.

[Rec17] Der österreichische Rechnungshof. Der Rechnungshof: Bundeskriminalamt. *Der österreichische Rechnungshof*, Mar 2017.

[Rec18] Der österreichische Rechnungshof. Der Rechnungshof: Bundeskriminalamt; Follow-up-Überprüfung. *Der österreichische Rechnungshof*, Jan 2018.

[RR96] Wolfgang Rentzel-Rothe. Elisabeth Bellmann, Die Internationale Kriminalistische Vereinigung. *Zeitschrift der Savigny-Stiftung für Rechtsgeschichte. Germanistische Abteilung*, 113(1):618–619, 1996.

[Sch12] Kristina Schöggl. Die polizeiliche europäische Zusammenarbeit nach dem Vertrag von Lissabon. Master's thesis, Universität Wien, 2012.

[Sol16] Daniel J Solove. A brief history of information privacy law. *Proskauer on privacy, PLI*, 2016.

[Sul99] Satish Sule. *Europol und europäischer Datenschutz*. Nomos-Verlag-Ges., 1999.

[Sup18] European Data Protection Supervisor. Interoperability between EU large-scale informations systems, Apr 2018. edps.europa.eu/data-protection/our-work/publications/opinions/interoperability-between-eu-large-scale-informations_en [Online; accessed 7. Apr 2019].

[Sup19] European Data Protection Supervisor. Annual Report 2018, Feb 2019. edps.europa.eu/sites/edp/files/publication/ar2018_en.pdf [Online; accessed 7. Apr. 2019].

[Tap96] Don Tapscott. *The digital economy: Promise and peril in the age of networked intelligence*, volume 1. McGraw-Hill New York, 1996.

[tCoCLJA09] The European Parliament the Committee on Civil Liberties Justice and Home Affairs. Public Seminar - An Efficient and Accountable Police Cooperation in the EU - the Way Forward, Dec 2009. europarl.europa.eu/meetdocs/2004_2009/documents/oj/643/643527/643527en.pdf [Online; accessed 25. Mar. 2019].

[Top18] Toppr. Digital Economy: Definition, Advantages, Disadvantages, Nov 2018. toppr.com/guides/business-environment/emerging-trends-in-business/digital-economy [Online; accessed 14. Mar. 2019].

[Tri12] Fair Trials. Interpol - Frequently Asked Questions, Jul 2012. fairtrials.org/node/1141 [Online; accessed 25. Mar. 2019].

[ttEU19] United States Mission to the European Union. Difference between a Regulation, Directive and Decision, Apr 2019. usda-eu.org/eu-basics-questions/difference-between-a-regulation-directive-and-decision [Online; accessed 24. Apr. 2019].

[TU 15] TU Graz | Austria-Forum. Polizei. *Austria-Forum*, Aug 2015. austria-forum.org/af/AEIOU/Polizei [Online; accessed 24. Mar. 2019].

[Uni12a] European Union. Consolidated version of the Treaty on the Functioning of the European Union, Oct 2012. eur-lex.europa.eu/eli/treaty/tfeu_2012/oj [Online; accessed 25. Mar. 2019].

[Uni12b] European Union. Consolidated versions of the Treaty on European Union and the Treaty on the Functioning of the European Union - Consolidated version of the Treaty on European Union - Protocols - Declarations annexed to the Final Act of the Intergovernmental Conference which adopted the Treaty of Lisbon, signed on 13 December 2007, Oct 2012. eur-lex.europa.eu/eli/treaty/teu_2012/oj [Online; accessed 30. Mar. 2019].

[Uni16a] European Union. European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (eu-LISA), Jun 2016. europa.eu/european-union/about-eu/agencies/eu-lisa_de [Online; accessed 12. Apr. 2019].

[Uni16b] European Union. European Union Agency for Law Enforcement Training (CEPOL), Jun 2016. europa.eu/european-union/about-eu/agencies/cepol_en [Online; accessed 30. Mar. 2019].

[Uni16c] European Union. The history of the European Union, Jun 2016. europa.eu/european-union/about-eu/history_en [Online; accessed 16. Mar. 2019].

[Uni16d] European Union. The history of the European Union - 1975, Jun 2016. europa.eu/european-union/about-eu/history/1970-1979/1975_en[Online; accessed 12. Mar. 2019].

[Uni16e] European Union. The history of the European Union - 1983, Jun 2016. europa.eu/european-union/about-eu/history/1980-1989/1983_en[Online; accessed 12. Mar. 2019].

[Uni16f] European Union. The history of the European Union - 1984, Jun 2016. europa.eu/european-union/about-eu/history/1980-1989/1984_en[Online; accessed 12. Mar. 2019].

[Uni16g] European Union. The history of the European Union - 1985, Jun 2016. europa.eu/european-union/about-eu/history/1980-1989/1985_en [Online; accessed 12. Mar. 2019].

[Uni16h] European Union. The history of the European Union - 1986, Jun 2016. europa.eu/european-union/about-eu/history/1980-1989/1986_en [Online; accessed 12. Mar. 2019].

[Uni16i] European Union. The history of the European Union - 1987, Jun 2016. europa.eu/european-union/about-eu/history/1980-1989/1987_en [Online; accessed 12. Mar. 2019].

[vL13] Klaus von Lampe. Was ist "Organisierte Kriminalität"? | APuZ. *bpb.de*, Sep 2013. bpb.de/apuz/168908/was-ist-organisierte-kriminalitaet [Online; accessed 24. Mar. 2019].

[WB90] Samuel D. Warren and Louis D. Brandeis. The Right to Privacy. *Harvard Law Review*, 4(5):193–220, 1890.

[Wik19] Wikipedia. Interoperabilität, Apr 2019. de.wikipedia.org/wiki/Interoperabilit%C3%A4t [Online; accessed 24. Apr. 2019].

[WW07] Werner Weidenfeld and Wolfgang Wessels. *Europa von A bis Z*. Nomos, 2007.

[Zie96] Frank Zieschang. Der Austausch personenbezogener Daten mittels Europol. *Zeitschrift für Rechtspolitik*, 29(11):427–429, 1996.