INTRODUCTION OF THE DATA PROTECTION REFORM TO THE JUDICIAL SYSTEM
INFORM

JUST-JTRA-EJTR-AG-2016
Action grants to support European judicial training
JUSTICE PROGRAMME
GA No. 763866

INtroduction of the data protection reFORM to the judicial system
INFORM

WP2: Data Protection regulatory review & training material elaboration

Review report on GDPR aimed at court staff

Lead partner: Masaryk University

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission. [1]

Project co-funded by the European Commission within the JUST Programme		
Dissemination Level:		
PU	Public	X
CO	Confidential, only for members of the consortium (including the Commission Services)	
EU-RES	Classified Information: RESTREINT UE (Commission Decision 2005/444/EC)	
EU-CON	Classified Information: CONFIDENTIEL UE (Commission Decision 2005/444/EC)	
EU-SEC	Classified Information: SECRET UE (Commission Decision 2005/444/EC)	
Document version control:		
Version 1	Originated by: Masaryk University	31/01/2018
Version 1	Updated by: Masaryk University, information regarding Bulgaria provided by Law and Internet Foundation	19/09/2018
Version 2	Rearranged and complemented by: Masaryk University, information regarding Slovakia provided by UNIBA, Appendix completed by INTHEMIS and University of Göttingen	22/02/2018
Version 2	Updated by: Masaryk University based on review by University of Göttingen	01/03/2018
Version 2	Reviewed by: Law and Internet Foundation	02/03/2018

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

Executive summary

On 25th May 2018 shall enter into force the European data protection reform package with General Data Protection Regulation 2016/679 as its main component. The regulation is focused on harmonisation and strengthening of personal data protection in the modern European society and brings therefore a number of innovative legal instruments and modified rules to the established European personal data protection landscape.

The INFORM Project is a cooperative effort of ten European partner organisations from Bulgaria, Cyprus, the Czech Republic, France, Germany, Hungary, Italy, the Netherlands, Poland and Slovakia funded by the European Commission under the Justice Programme 2014-2020. Its focus is to contribute to the effective and coherent application of the General Data Protection Regulation 2016/679 and the Directive 2016/680 by the target groups, which are the judiciary, legal practitioners, and the court staff.

The following report provides an in-depth review into the particular aspects of General Data Protection Regulation with respect to the tasks and activities performed by the court staff. Given the differences between the particular organisational structures of the judiciary in the Member States the term "court staff" is analysed in detail and a scope of definition for the purpose of this review is found. In the following section are described the particular tasks and activities of the identified court staff that may present a form of personal data processing. The latter sections then focus on particular obligations or rights pursuant to General Data Protection Regulation and their assessment in context of court staff personal data processing activities.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

Table of contents

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

List of Abbreviations

AI	Artificial intelligence
CEPEJ	European Commission for the Efficiency of Justice
CJEU	Court of Justice of the European Union
DDoS	Distributed denial of service
DG	Directorate-General
DPA	Data protection authority
DPIA	Data protection impact assessment
DPO	Data protection officer
ECHR	European Court of Human Rights
ENISA	European Union Agency for Network and Information Security
EU	European Union
GDPR	General Data Protection Regulation
HR	Human resources
ICT	Information and communication technology
IP	Internet protocol
IT	Information technology
MS	Member State

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

Chapter 1: Scope and definition of the court staff

The rule of law essential to modern democratic society depends largely on proper functioning of the judicial system. This on the other hand relies on effective cooperation between the judiciary and those responsible for administration of the courts.[1] Court staff therefore represents a vital role that merits a focused in-depth analysis.

The general EU-wide approach to definition of the court staff category is very problematic, because the framework organisation of court system is different in each Member State.[2] Furthermore, the perception and particular organisation of the court staff differs between the Member States, leading to a broad variety of different functions within different systems.[3]

Court staff represents a body of court personnel, who alongside judges provide a crucial component of functioning judicial system. These professionals possess particular knowledge of the case-flow management, requirements for legal court procedure, back-office management of the court room and many other essential processes of the court. During these various operations they frequently come in close contact with sensitive and intimate details about parties to the proceeding, witnesses or third persons as well as about the court personnel. Vast majority of these operations present a form of personal data processing that is regulated by GDPR.

To properly consider these various operations of the court staff, the accepted scope and definition of this category must be reasonably broad and inclusive.

One such broad perception was suggested by Oertel and Goldschmidt under the DG-Justice funded project *Study on the state of play of court staff training in EU law and promotion of cooperation between court staff training providers at EU level*.[4] It reflects upon the broad variety of court staff functions according to the

[1] Wayne Martin, 'Court Administrators and the Judiciary — Partners in the Delivery of Justice' (2014) 6 International Journal for Court Administration <http://www.iacajournal.org/articles/abstract/10.18352/ijca.158/> accessed 28 January 2018. p. 3.
[2] Roberta Ribeiro Oertel and Peter IB Goldschmidt, 'The Training of Court Staff and Bailiffs at the European Union Level' in Directorate-General for Internal Policies of Union (ed), *The Training of Judges and Legal Practitioners* (European Parliament 2017) <http://www.europarl.europa.eu/RegData/etudes/IDAN/2017/583134/IPOL_IDA(2017)583134_EN.pdf>. p. 41.
[3] *Ibid.* p. 40.
[4] *Ibid.* p. 42.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

factsheets provided by responders from the Member States[5] and attempts to aggregate the broad range into three core functional categories.

The category *Functions related to the administration and management of Courts* is meant to cover the general administrative role of court personnel and its basic operations, including: general management; human resources; facility management; e-justice implementation; organisation of legal registries; providing information about access to justice and legal aid; administration of ICT systems and their maintenance; budget and bookkeeping; court programming and secretariat functions.[6] Alongside these roles the authors of the study consider the category *Judicial functions*, which could be perceived as the narrow scope of court staff definition. Here should be included the enforcement of court decisions; service of judicial and extra-judicial documents; assistance to judges; as well as judicial and/or procedural decisions in specific cases and/or fields of law.[7] The third category involves the *Procedural functions* of the court staff, including cross border judicial cooperation, particularly completing requests to courts in other countries or receiving such requests, as well as observance of procedural rights in criminal cases.[8] This categorisation provides a practical overview of the general scope of the court staff category, which can serve as a basis for further analysis in a greater detail for the purpose of assessment of personal data processing by the court staff.

Additional definition of court staff can be derived from reports by European Commission for the Efficiency of Justice (CEPEJ). Here the basic distinction is between five types of non-judge staff with some mode detailed information on the specifics of each reporting state. The first specific role that is to be distinguished is the function of "*Rechtspfleger*"[9], meaning the high-ranking judicial officials to whom judicial tasks have been transferred, who therefore work independently alongside judges and have capacity to issue judicial decisions in certain categories of cases. Other type of non-judge staff is those, who assist judges directly. This includes judicial advisors and registrars. Third type covers the

[5] Available at <https://e-justice.europa.eu/content_court_staff_s_training_systems_in_the_member_states-408-en.do>
[6] Oertel and Goldschmidt (n 2). p. 42.
[7] *Ibid.* p. 42.
[8] *Ibid.* p. 42.
[9] This category is represented by the European Union of Rechtspfleger (E.U.R.), a non-governmental organization enjoying participatory status with the Council of Europe and functioning as observer at the CEPEJ. Homepage available at: <http://www.rechtspfleger.org/en/>.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

general court staff responsible for administrative matters and court management. Fourth are the members of technical staff responsible for IT equipment, security and cleaning. The ultimate type reflects the diversity of the national systems, allowing for inclusion of other non-judge staff that does not fall in the previous categories.[10]

The above-mentioned role of "*Rechtspfleger*" or equivalent staff is present in the judicial systems of twelve Member States.[11] Kappl, the former president of the European Union of Rechtspfleger, described their role as analogy to a senior court officer who replaces the judge in limited areas of the law, but with wide ranging functions.[12] There is, however, noticeable disparity in the specific roles of these court officials. They can be identified as judicial officers with a special training and qualification (Austria, Germany, Poland, Romania, Slovenia), senior judicial officers deciding simple matters and keeping record (Czech Republic, Slovakia), specific function with judicial authority (Spain), functional alternative to deputy judges (Denmark), assistant judges (Estonia), court clerks (Hungary), authorized land registry officers (Croatia), as well as county registrars (Ireland).[13]

The data available from Member States in the aforementioned CEPEJ report do not specify to a necessary degree the particular composition of the non-judge staff that assist the judge directly, the general staff or the technical staff, as it is focused primarily on quantitative indicators (number of non-judge staff, variation, gender distribution etc.). Furthermore, as stated by Holvast, there is remarkably little knowledge regarding the role of court staff in most judicial systems outside of the United States.[14] For this reason, the following description is based on available information from Czech judicial system,

---

[10] CEPEJ, 'European Judicial Systems Efficiency and Quality of Justice. CEPEJ STUDIES No. 23. Edition 2016 (2014 Data).' <https://www.coe.int/t/dghl/cooperation/cepej/evaluation/2016/publication/REV1/2016_1%20-%20CEPEJ%20Study%2023%20-%20General%20report%20-%20EN.pdf>. p. 146.

[11] CEPEJ, 'Study on the Functioning of Judicial Systems in the EU Member States. Facts and Figures from the CEPEJ 2012 -2014 Evaluation Exercise'
<http://ec.europa.eu/justice/effective-justice/files/cepj_study_scoreboard_2014_en.pdf>. p. 231.

[12] Thomas Kappl, 'Guest Editorial: Strong Justice for a Strong Europe: A European Rechtspfleger' (2016) 8 International Journal for Court Administration <http://www.iacajournal.org/articles/abstract/10.18352/ijca.212/> accessed 28 January 2018. p. 1.

[13] CEPEJ (n 11). pp. 232-235.

[14] Nina Holvast, 'The Power Of The Judicial Assistant/Law Clerk: Looking Behind The Scenes At Courts In The United States, England And Wales, And The Netherlands' (2016) 7 International Journal for Court Administration <http://www.iacajournal.org/articles/abstract/10.18352/ijca.200/> accessed 28 January 2018. p. 11.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

with an assumption that the main roles of these categories should not differ to a degree that would make further assessment of personal data processing invalid.

The composition of the core court staff has to understandably differ between various judicial branches and instances, as the necessary administrative positions vary in consequence of the particular operations of the court. If we are, however, considering the probable common structure of a court organisation, the following functions may be identified as falling within the court staff category. Of particular importance are all operations that directly come into contact with the court files, evidence or other documents or information essential for the court proceeding. First instance with this function is the filing office of the court, which is responsible for the reception and posting of multitude of court documents. An indispensable role in the court proceeding is then played by the clerks and registrars, who provide various supporting functions to the judge during the proceeding, including the record keeping. The central administration of court files is usually provided by the registry of the court files, which inter alia ensures documentation of the location, access and contents of the court files. Exceptions are court files containing classified information, which are usually managed by the security office of the court. Parallel to this registry may some courts operate also an evidence and record keeping department that serves either as archive or as a registry for the evidence relevant to the court proceedings.

Additional to the aforementioned court staff directly assisting the judge or handling the court files, there are numerous functions and roles that provide indirect support to the court operations. Most importantly, the predominant number of courts includes an IT-department with administrators of court information systems, networks, databases and applications. The role of these is highly dependent on the achieved level of e-justice, but it can be certainly assumed that all courts nowadays operate to some degree with the help of information and communication technologies. Wallace notes that impact of technology on the courts is a topic for nearly three decades now; however, there was a recent shift in the discussion. Previously the dominant topic was the impact of technology on the way that courts carry out their role (e.g. courtroom technology), but greater attention is now being paid to the way that

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

technology may affect the nature of the work that the legal profession and the courts undertake in the future (particularly the automation and the role of AI).[15]

The management of a court is usually performed by the president of the court, who is in these tasks supported by secretariat or president's office as well as standard departments like the human resources, public relations or economic departments. Some higher courts also have an analytical department that analyses the available case law and organizes the training and education of judges and judge assistants. Alternatively some of these functions can be performed by the court library.

As to the other non-judge staff, various Member States report particular functions that fall within their perception of court staff that are not similarly reflected in other Member States. To better illustrate the variety, several examples follow: judicial trainees, people in charge of serving court documents (on the parties), press centre and telephone exchange (Czech Republic); court interpreters (Estonia); assistants, receptionists, porters (Italy); translators (Lithuania); assistance magistrates, judicial assistants, probation counsellors (Romania).[16]

Notwithstanding the above mentioned, there remain functions of staff at the courts of Member States that are bordering the scope of court staff definition, but for some reasons are difficult to consider under the above mentioned categories. First example is the judicial guard (marshals), who process personal information *inter alia* through the record of visitors to the court. The members of the judicial guard generally follow instructions by the judges, but are not employees of the court (mostly they are members of a specifically designated policing unit).

In multiple Member States the court structure includes assistant or trainee judges, who are not comparable with the court staff, as their mandate and authority is largely reflecting their role as future judges (to significantly larger degree than it is the case by the "*Rechtspfleger*"), but who are no judges *per se*. Given the close link between the functions of judge assistants/trainees and professional judges,

[15] Anne Wallace, 'The Impact of Technology on Courts' (2017) 8 International Journal for Court Administration <http://www.iacajournal.org/articles/abstract/10.18352/ijca.236/> accessed 28 January 2018. p. 1.
[16] CEPEJ (n 11). pp. 256-258.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

there seems to be limited justification for including this group under the court staff category instead of judiciary.

Particularly higher courts also often employ consultants or expert advisors for specific areas of law. These persons usually have a contractual relation with the court as employees, their inclusion in the perception of court staff is, however, misleading, as their role remains limited to providing the judges or judge assistants with on-request advice or consultation (they are also unlikely to process personal data in a significantly different way than the already considered court staff roles).

Similarly unfitting would be to consider under the court staff category various student aids or interns, who do not represent an essential component of the court operations, but perform a rather auxiliary function focused primarily on their own experience and education rather than proper functioning of the court.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

Chapter 2: Material scope of application of the GDPR with respect to court staff

The aforementioned scope of the term "court staff" needs to be perceived for the purpose of this report particularly with regard to the operations that constitute personal data processing under the scope of application of GDPR. The data protection reform follows the basic concepts of the Data Protection Directive 46/95/EC and continues the progress towards a unified approach to data protection. The variety of approaches to the institutional organisation of judicial bodies in the Member States necessitates open formulations in the European level legislation that shall be further specified in national law. Due to the role of judiciary as the public system of dispute resolution and pursuit of justice, many fundamental principles of personal data protection required by GDPR are inherent to the existing operational and functional framework of the judicial system. The tasks of the court staff are incorporated in this structure and often the particular operations or activities described in this report need to be considered in this context and their assessment needs to reflect the broader systematic organisation of the court or judiciary as a whole.

2.1. Processing wholly or partly by automated means or part of a filing system

The processing takes automated or semi-automated form particularly through employment of information and communication technologies. These are gradually incorporated into the judicial system through the agenda of e-justice and nowadays can hardly any court function without any form of ICT support. The primary form of processing through ICT technology is the use of office technology (software with auto-filled forms, analytical software, proceeding monitoring software, statistical analysis of the file-flow and workload, voice recognition used for document creation, electronic communication with the use of electronic signatures etc.).[17] Personal data may also be

[17] Dory Reiling, 'Technology In Courts In Europe: Opinions, Practices And Innovations' (2012) 2012 International Journal For Court Administration. p. 5.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

processed through ICT during the hearings, e.g. by videoconferencing, video and audio recording or manipulation and projection of (electronic) evidence.[18]

Many forms of administrative manipulation with the court files are either recorded or partly automated, whereas this holds particularly true for the e-filing system. Related forms of processing by the court staff are then operations with the court evidence or case law databases, particularly during independent judicial tasks of the "Rechtspfleger" subcategory.

Similarly to any other organized body or institution, there are numerous administrative and organizational tasks and processes that are carried out by the court staff in the relation to the day-to-day functions of the court (human resources management, financial and budgetary operations, public relations releases, reception, secretariat or IT-maintenance tasks etc.). Despite many of these operations being cases of personal data processing, they are mostly auxiliary to the main focus of this report, as there is usually little difference from similar operations by other public or private entities.

2.2. Scope of application in comparison to Directive 2016/680

GDPR as the general regulatory framework for personal data protection applies by default to all forms of personal data processing within the operations of the court, unless stipulated otherwise, particularly in case of specific national or European legislation. The Directive 2016/680 represents such specific regulation with regard to prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security. GDPR therefore shall not apply to personal data processing that is part of the criminal proceedings in the court agenda and all related operations. For this review are therefore also irrelevant the activities of state prosecutors and their respective office staff in the context of criminal proceedings. Despite this attempted narrow focus disregarding the Directive 2016/680, the internal structures of court staff organisation may not always reflect this legislative distinction. Various court staff tasks bordering the judicial capacity of the court may be performed jointly for both civil and criminal proceedings (e.g. management of ICT, HR, the registry office, cash register or archive).

[18] *Ibid.* p. 6.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

Apart from criminal proceedings, some Member State jurisdictions also recognize specific form of disciplinary proceedings, e.g. for disciplinary offences by judges or bailiffs, which to a large degree follow the procedural rules of criminal proceeding, do, however, not aim towards sanctioning of the offenders according to the principles of material criminal law, but rather substitute and formalize professional accountability for these particular positions that are generally endowed by functional independence of their post. As these disciplinary proceedings cannot be fully qualified as a form of criminal proceeding, it must be assumed that the personal data processing related to these proceedings is governed by GDPR, unless the Member State legislation provides otherwise.[19]

2.3 Specific MS legislation regarding courts and judicial authorities

Personal data processing as part of the activities of courts and other judicial authorities is met with particular requirements for safeguarding of the independence of the judiciary and its performance of judicial tasks. This distinction is recognized by the GDPR framework and the Member States are entitled to specific national legislation regulating the personal data processing in this scope.

Currently, no overall analysis in this regard can be provided, as many Member States did not yet complete the adoption of such specific legislation and some are still only in the early phase of drafting such legislation.

The Czech Republic is among the Member States with the longest legislative path still to be taken for the specific national legislation to be adopted. The currently available *Návrh zákona o zpracování osobních údajů* (draft Act on Personal Data Processing) and *Návrh zákona, kterým se mění některé zákony v souvislosti s přijetím zákona o zpracování osobních údajů* (draft Act to Amend Some Acts Pursuant to the Adoption of Act on Personal Data Processing) provide an early basis for the specific examples that shall be provided in further sections in order to be able to analyse the described features of personal data processing by the court staff in more detail.

In Bulgaria at the moment of finalization of this review, there is no legal act or draft of a legal act transposing GDPR into the Bulgarian legislation. The pertinent law – the Judicial System Act (JSA)

[19] Recital 20 GDPR.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

and its adjoining Rules regulate the activities of both judiciary and judicial administration. In view of the specific scope of this review it should be noted that in Bulgaria the management of the administrative activities is executed by the Court chairman, who is a magistrate. However, when it comes to the actual implementation of the administrative functionalities, it is the administrative personnel, also referred to as court staff under the INFORM project, that is responsible for it. Furthermore, the national legislator has exhaustively listed the functions of both court staff and judiciary, and their thorough examination shows that there is no overlapping and ambiguousness.

In Slovakia, there was adopted a specific act No. 18/2018 Z. *z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov* (Act on personal data protection and on amendment and complementation of selected acts), which shall come into force on 25th May 2018. Other significant legal acts relevant to assessment of the organisational and structural framework of Slovak court system and role of the court staff include; *Zákon č. 757/2004 Z. z. o súdoch a o zmene a doplnení niektorých zákonov (*Act on courts and amendment and complementation of selected acts), *Zákon Národnej rady Slovenskej republiky č. 38/1993 Z. z. o organizácii Ústavného súdu Slovenskej republiky, o konaní pred ním a o postavení jeho sudcov* (Act on organisation of the Constitutional court of the Slovak republic, on proceeding in front of this court and on status of its judges), and Spravovací a rokovací poriadok uverejnený pod č. 114/1993 Z. z. v znení ďalších zmien a doplnkov (Administrative and procedural [court] order).

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

Chapter 3: Data type and data processing activities performed by court staff

The particular scope to which the members of court staff become involved in operations representing processing of personal data is to a large degree dependent on the location, specialisation, national jurisdiction and instance of the court concerned. There are, however, numerous components of the typical operations of the court staff that are in the essence similar to most judiciary systems considered and can thereby be assessed as relevant for the purpose of this report.

An aspect that needs to further be taken into consideration is that court staff in most cases processes personal data as part of their employment obligations towards the court, there is therefore limited space for consideration of the data controller or processor question, as the court staff is mostly acting under the authority of the court,[20] irrelevant if the court acts as data controller or processor. Given the specific role of judiciary it can further be assumed that most tasks that constitute personal data processing should be initiated and govern through the court as data controller and not a third entity. An exception may be aspects of judiciary administered by other governmental body (e.g. Ministry of Justice) or processing based on request within the judiciary (direction or request between instances/courts or cross-border request for cooperation). However, even these instances are mostly to be perceived as situations with multiple joint controllers or instances of the court acting as recipient of personal data and controller with regard to its further processing.

Further aspect to be considered, which was already mentioned in the previous section, is the implemented level of e-justice mechanisms. An assessment of a functionally similar operation (e.g. keeping record of individuals, who accessed the court file) can greatly differ, if it is performed only in the written form by the authorized court staff, in a form of localized offline digital chart managed by authorized court staff and court IT-department or through a customized automated e-file management

[20] The regime of Article 29 GDPR.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

system provided by verified third party and administered by department of executive governmental body (e.g. Ministry of Justice).[21]

3.1. The requirement of personal data and its limits

3.1.1. Notion and content

The notion and content of the term personal data was explained in accordance with the new European data protection reform for the purposes of this project in the previously delivered Glossary.[22] Furthermore, the personal data processed by the court staff mirrors the categories that are processed by judiciary as a whole. It would therefore be rather repetitive to provide additional interpretation of this term as part of this review. For more information, please consult D2.1 Review report of GDPR with respect to judiciary, developed under the INFORM project.

3.1.2. Pseudonymisation and Anonymisation

Both anonymisation and pseudonymisation are terms well established in the European personal data protection law. Anonymisation presents a process that transforms the personal data into information, from which an identification of the data subject is no longer possible.[23] Pseudonymisation in contrast is a safeguard for storage and processing of personal data in a modified form that requires for identification of natural person additional information, which is kept separately.[24] Pseudonymisation techniques are applied to various direct identifiers in court documents made accessible to the public. It is also a measure that may be suitable for certain types of internal databases, e.g. logs of court file access or access authorization catalogue.

[21] European Commission for the Efficiency of Justice, 'Use of Information Technology in European Courts - CEPEJ Study No. 24' 24 <http://www.coe.int/t/dghl/cooperation/cepej/evaluation/2016/publication/CEPEJ%20Study%2024%20-%20IT%20report%20EN%20web.pdf> accessed 4 July 2017. p. 41-42.
[22] University of Cyprus, 'INFORM Project Deliverable D2.11 Data Protection Glossary'. p. 31.
[23] Article 29 Data Protection Working Party, 'Opinion 05/2014 on Anonymisation Techniques 0829/14/EN WP216' <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf> accessed 28 January 2018. p. 5.
[24] University of Cyprus (n 22). p. 37.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

The Member States have a different approach to application of anonymisation and pseudonymisation techniques to publicly available court documents, particularly to the publicly available court decisions. The GDPR regulatory framework does not provide guidance in this regard; it is therefore a matter of national legislation, tradition and practice that define adequate standard for publication of court documents and their anonymisation.

Nevertheless, manipulation with the court documents, correspondence, registries, recordings of proceedings and many other tasks of the court staff require access to data with full content and detail. Overall zeal in internal pseudonymisation would increase the burden on court administration, decrease the effectivity of court processes and affect the quality of performance by the court staff. It is therefore necessary to prioritize other measures for adequate protection of personal data processing, e.g. encryption.

3.1.3. Critical cases regarding the data processing of court staff

The potential categories of personal data that may be processed by the court staff during their tasks are mainly connected to the identification, verification of identity or claim, authorization and communication with or to a third subject or entity. As one of the roles of court staff is to assist the judge, the scope and form of personal data processing may differ depending upon the assistance required (collection of data, analysis of court file, verification of document validity, transcription or summarization of evidence or registry information, protocol and record keeping etc.).

3.1.4. Special types of data and the consequences for data processing

The processing of special types of personal data is not perceived as systematic part of most court staff tasks, it can, however, not be ruled out, as the contents of the court files and supplementing document are based on the nature of the dispute and proceeding. Particularly the record keeping of the proceedings may therefore constitute a form of processing that may include any category of personal data, depending upon the subject-matter of the proceeding and dispute.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

Apart from court file and evidence the court staff may come into routine contact with biometric data[25] through identification of witnesses, expert witnesses, parties to the proceedings or visitors and personnel in the court premises. This task, however, mostly falls to judicial guard or bailiffs, who (as described in section above) are not easily recognizable as constituent part of the court staff term. Yet it cannot be dismissed that other court staff personnel does not come into contact with biometric data under similar circumstances. Example may be the security office of the court, Rechtspfleger or other functions that are likely to process such sensitive personal data as part of their work tasks. This may to certain degree be assumed also with respect to genetic data,[26] an occurrence of such processing is, however, unlikely. Data concerning some aspects of health[27] of the court personnel may be available to HR department or court administration, these should, however, by default not be accessible to these instances under regular circumstances.

Court staff may also stand on the other side of the equation as the data subject. Various security measures in the court premises or on the court equipment may be secured through access control with biometric authorization. Such measure would constitute personal data processing that would require legal basis pursuant to Article 9, most likely an explicit consent by the court staff.

3.2. Activities of data processing

Given the broad spectrum of operations that fall under the above defined functions of court staff, it is appropriate to expect that the data processing can in various situations within these functions take form of a wide variety of data processing activities.

The particular form, purpose and scope of these activities largely depend on the task entrusted to the court staff and the instance and form of proceeding that it relates to. Majority of the general administrative functions of court staff take place irrespective of the particular agenda or jurisdiction of the court. Their judicial or procedural functions do, however, often differ in this regard depending on the particular court or proceeding.

[25] *Ibid.* p. 9.
[26] *Ibid.* p. 26.
[27] *Ibid.* p. 17.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

Some proceedings are closely linked to the processing of data in public databases, like commercial, trade or land register. Other involve numerous intimate and sensitive personal data, like proceedings dealing with divorce, parental care, protection from domestic violence, determination of parenthood, adoption and similar matters. Similarly, there are multiple forms of civil proceedings regarding unwarranted interference in personal rights, e.g. privacy, non-discrimination, dignity, good reputation, personal freedom or physical or mental integrity. Even if the members of court staff are not directly deciding these cases, their supporting role in the judiciary operations means they come into contact with personal information processed in these proceedings. Often it is the task of the court staff to record, analyse, summarise or collect such information in order to assist the judge with the case.

There are multiple other forms of civil, administrative, or disciplinary proceedings that involve processing of specific types of personal data (often related to financial assets, employment, education, family, habits, activities, political or religious views, labour union membership etc.) about data subjects, whereas the scope and detail depends on the *ad hoc* parameters of the case. Nevertheless, it is to be presumed that assigned members of the court staff will have access to majority of personal data processed during such proceeding as part of their various tasks and activities that ensure proper procedural progress in the case and that assist the judge with the management of the proceeding and preparation of the ruling.

3.2.1. Collection

The collection of personal data is not primary modus operandi of judicial system, there are, however, instances of this activity. Personal data is collected about the parties to a proceeding, about the visitors to the court building, about the court staff and judges as part of the general administrative operations as well as during analytical and statistical evaluations of the court functions.

3.2.2. Recording and storage

Personal data are being recorded particularly during hearings by the authorized registrar in the record of the proceeding. Further data is also recorded in the filing office upon reception of new submissions or mail. General administrative activities also include instances of recording, e.g. security cameras in

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

the building of the court, protocols of access and location of the court files, operations with the received mail and documents.

Storage of personal data is one of the most important forms of personal data processing in the context of court staff activities. The proper functioning of the court on a daily basis as well as the observance of principles of fair trial and effective judicial system require extensive documentation of received and processed information. Stored are *inter alia* protocols, files, evidence, logs, or transcripts of the hearings. The personal data storage can be modified through the adoption of e-justice platforms, particularly the e-filing system and cloud or local back-up.

3.2.3. Organisation and structuring

Combination and categorisation of personal data is not the primary goal in most operations of the court staff, it does, however, play a role in some general administrative operations like human resources management or procedural ensuring of fair trial (verification of the witnesses, processing of the court files, documentation of the court hearings, statistical analysis of the case-flow etc.). Furthermore, organisation of the file system and classification of the corresponding documents and submissions requires structured processing approach.

3.2.4. Adaption or alteration

The alternation of personal data takes place primarily as a result of a notification by the affected subject about a change or alternation of relevant information in the court file or accompanying documents. The update of personal data must be often reflected in several protocols or files. Particular instance of alternation of personal data is then the change of record in public registries administered by courts (e.g. commercial registry). Alternation of recorded personal data is occasionally also necessary due to mistakes and conflicts between different agendas or miscommunication between court instances or departments.

3.2.5. Retrieval or consultation

The personal data is often retrieved from the submitted files or documents for the purpose of record keeping and analysis. Stakeholders may be requested to supplement the submitted personal data or can be consulted about their validity and specific content.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

3.2.6. Use

Personal data are used by the court staff to assist the judge, verify the authenticity of the documents, ascertain the identity of the subject or research the validity of the information. It is further used according to the instructions of the judge or during the addition of the clause of legal force.

The process of sending court documents and other communication also requires use of personal data of the receiver or affected parties. Also the distribution of received mail to the respective recipients within the court results in personal data processing. Documents with such data may also need to be conversed, if received in electronic form with electronic signature.

3.2.7. Disclosure by transmission

The personal data processed as part of the proceeding are communicated to the parties or other stakeholders in the dispute. Courts as public bodies are subject to national legislation concerning free access to information. Such disclosure may be either routine (e.g. publication of court decisions online) or per request. Data can be further disclosed to courts from other countries based on requests within the cross-border judicial cooperation. These countries may include also third countries outside the Member States.

3.2.8. Dissemination or otherwise making available

Publication of court decision or distribution of other public relation information can be also considered part of the court staff activities agenda. Also administration of public registries is a form of dissemination of personal data to broad public. Courts should further communicate basic information about proceedings to the media and public, there is therefore usually a public relations officer managing this form of communication (particularly by higher courts). There are rules in place for the minimization of personal data disseminated through the publication of court decisions, these may, however, not always meet the necessary standard for adequately anonymised or pseudonymised data. Furthermore multiplication and printing of various court documents can take form of internal or external dissemination.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

3.2.9. Alignment or combination

Combination of information is part of the process behind creation and update of court file and supporting documentation. In case of a lost or destroyed file, a reconstruction through combination of available information may be attempted.

3.2.10. Restriction

Restricted regime of data processing may be established by specific legislation, e.g. in case of court files containing secret information or in case of proceedings with vulnerable data subjects (parental responsibility cases, legal capacity limitation etc.).

3.2.11. Erasure or destruction

According to specific legislation, the stored files and evidence may need to be destroyed after a passage of time. Furthermore, appropriate erasure and limitation of storage with accordance to the legal requirements must be ensured in the digital systems and databases of the court.

3.3. Who is data controller and who is data processor?

3.3.1. Notion

As already outlined in the beginning of this section, the identification of data controller and data processor is from the perspective of court staff processing rather secondary, as the members of court staff are employees of the court and thereby act under the authority of the court. Taking into consideration the general requirement of functional and institutional independence of the judicial system it is to be presumed that generally the court will act as data controller and only a limited number of operations may be delegated to a separate data processor.

3.3.2. Critical cases regarding court staff

There are some areas that provide particular setting that makes the identification of data controller relevant to the assessment of court staff operations. Firstly, if the processing takes place through an e-justice platform, there can potentially be added complexity due to the role of developer and administrator of the system. This is connected to the situation present in some Member States, caused by imperfect separation of judicial and executive branches (i.e. national systems that lack an

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

independent judicial administration body in form of a council for judiciary). In such cases, the government (e.g. through the authority of the Ministry of Justice) may to some degree administer and determine various operations within the judicial system that are related to the general management, procurement and administration. If such operations include e.g. human resources management, financial and budgetary administration, maintenance of IT-system and databases (e.g. central online registry for correspondence, central cybersecurity measures or sectoral proxy server for internet access) or implementation of e-justice, then the issue of the role of the data controller and data processor becomes increasingly relevant. Nevertheless, most instances are likely to constitute the setting of joint controllers rather than controller and processor, as both executive and judicial bodies exercise certain portions of control over the operation.

Additional examples are the national or international transfers of court files between courts or requests between courts for performance of certain action in the court proceeding. These cases, however, also most likely constitute a relation between two controllers, as the recipient court processes the transferred personal data within its capacity in accordance with its institutional independence.

The information systems by the Czech courts are an example of the above described complex scenario. Currently there are various information systems implemented throughout the Czech judicial system, with the highest courts featuring specific customized information systems, which compatibility with systems of the other courts is limited. The systems of lower courts are partially administered with the help of the department in the Ministry of Justice; therefore, the scenario of joined controllers is likely. Additionally, the electronic filling office system, used mainly for the specific Czech electronic communication tool, the data box, which is an electronic storage site intended for delivery of official documents and for communication with public authority bodies, is centrally managed by the Ministry of Justice and only then further distributed to the corresponding court data boxes, i.e. electronic filling offices.

The courts in Bulgaria employ dedicated personnel to take care of the information systems. The Information security officer is the one who maintains the classified information protection and is directly subordinated to the Court chairman. Furthermore, as the Supreme Judicial Council is the

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

public body bound to manage the Bulgarian judicial system, it should be noted that there is a dedicated Directorate "Information technologies and judicial statics", where there is a department "Information services to the judicial authorities".

With regards to the issues of the correlation of the principle of judicial independence and the e-justice systems, it should be taken into account that currently in Bulgaria there is no e-justice system. However, several electronic services are available, whereas the IT system for random distribution of cases to the judiciary should be noted. The IT system was conceptualised in a manner that respects the principle of judicial independence.

Also in Slovakia are the information systems of the courts administered in cooperation with the governmental ministry. The ministry manages a central information system.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

Chapter 4: Fundamental principles relating to processing of personal data under GDPR

Reflecting the purpose and aim of the personal data protection framework, the core requirements are expressed in the form of fundamental principles, which similarly to other legal norms guide and facilitate interpretation and application in individual cases.

Pursuant to Article 5 the processing must proceed lawfully, fairly and in a transparent manner in relation to the data subject on principle for specified, explicit and legitimate purpose. The scope of processed personal data must be adequate, relevant and limited to what is necessary in relation to processing purposes. Every reasonable step must be pursued to process accurate and, when necessary, up to date personal data and allow timely erasure or rectification of inaccurate personal data. The storage of non-anonymised personal data is in principle permitted only for timeframe necessary for purposes of the processing. Adequate measures shall be taken during the processing to ensure appropriate level of security and protection from unauthorised or unlawful processing, as well as accidental loss, destruction or damage. The controller shall be responsible for the processing fulfilling these core requirements and shall be able to demonstrate compliance in this regard.

The principles of personal data processing pursuant to Article 5 are described in detail in the Appendix to the current review. The application of these maxims on the operations of court staff cannot be in principle separated from the broader implementation in the judicial system as a whole. As such, they are reflected in further consideration of specific requirements and situations relevant for this report.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

Chapter 5: Lawfulness of processing

5.1. Legal basis pursuant to Article 6

The basis for lawfulness of processing within the operations of court staff can also largely be related to assessment regarding the judiciary as a whole. The judicial system presents a vital branch of the state structure, performed by public bodies established through law. As such, the jurisdiction and authority of courts is defined and based on the law and represents primarily an exercise of public authority. The main basis for lawfulness of personal data processing through the court can therefore be seen in Article 6 para. 1 lit. e, as the necessary processing for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. The lawfulness of processing through the court staff, considering the broad understanding of this term presented in previous sections, derives from the legal basis of processing applicable to the operations of the controller, i.e. the court. The primary relationship between the court staff and the court is based upon an employment contract, which leads to the application of Article 29. The members of court staff are therefore in this regard to be perceived as persons acting (within the bounds of their assigned tasks as employees) under the authority of the court, disregarding the need for qualification, if the court acts with regard to given processing as the controller or the processor.

The other legal basis under Article 6 are less likely to be applicable to the performance of the main task of the judiciary, they should, however, not be omitted with regard to some supporting or auxiliary roles of the court staff. The requirement of consent from the data subject under Article 6 para. 1 lit. a can often be the only basis for communication of personal data about the court employees or parties to a dispute to the media or on the website of the court. Consent may also be required for some detailed forms of analytical or statistical processing aimed at an increase of efficiency of the judicial system or better management of the court premises. It must, however, be noted, that the application of consent in the processing of personal data by judicial bodies is limited due to the imbalance of

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

power.[28] Similar issue of imbalance of power and therefore potentially not freely given and thereby invalid consent occurs with respect to the processing of personal data of court staff, as they are in employment relationship with the court (as data controller).[29]

The application of Article 6 para. 1 lit. b can be relevant with regard to personal data required from the court personnel for the management of human resources. Compliance with a legal obligation to which the controller is subject pursuant to Article 6 para. 1 lit. c is to be considered as valid legal basis for activities of the court staff that are not directly related to the performance of judicial authority by the court and therefore the link to public interest or exercise of public authority is more difficult to establish. Article 6 para. 1 lit. f may apply to prolonged storage of personal data about former members of court staff.

5.2. Legal basis pursuant to Article 9

With respect to processing of special categories of personal data pursuant to Article 9 should be noted the exception included under para. 2 lit. f. The processing of these sensitive personal data is therefore lawful within the scope of judicial capacity of the given court. It is thereby defining to delimit the scope of judicial capacity; however, this assessment cannot be performed with sufficient detail on the level of abstraction that is prerequisite for this report. The particular landscape of judicial capacity depends on specific national legislation and organization of judicial system, as well as specific role and functions of the given court in such a national system. Pursuant to recital 20 and particularly more general requirements bound to independence of judicial system as well as fundamental rights to a fair trial and to an effective remedy and judicial protection, the scope of judicial capacity should be perceived in a broad sense, i.e. including all activities that are related to the effective functioning of the judicial system in accordance with its purpose.

Following this argumentation, broad scope of activities pursued by court staff as part of their various work tasks should be perceived as performance within the scope of judicial capacity of the court and

[28] Recital 43 GDPR as well as Article 29 Data Protection Working Party, 'Guidelines on Consent under Regulation 2016/679. 17/EN WP259'. p. 7.
[29] *Ibid.* p. 8.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

thereby covered by the exception of Article 9 para. 2 lit. f. This conclusion should be seen in the relative perspective of more general adequacy balancing, meaning that the scope of judicial capacity exception should apply only to adequate processing of special categories of personal data relevant to the court proceeding or other court activity with the sensitivity of such personal data being taken into consideration.[30]

The court staff does also process special categories of personal data related to other members of the court personnel within its auxiliary functions. These processing should be primarily connected to the administrative aspects of the internal organization of the court, e.g. management of human resources and their respective suitability for various roles within the court personnel hierarchy. Such processing should be covered by exception under Article 9 para. 2 lit. b, aimed at processing necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law within the legal bounds and with appropriate safeguards for the fundamental rights and the interests of the data subject in place. The versatility of roles that are considered under the term of court staff within European Union does not allow for closer assessment of specific requirements connected to these roles. It can, however, be assumed, that requirements of personal integrity, impartiality or professionalism are put in place for majority of court staff functions, given the responsibilities and authorizations bound to these professions.

[30] Boris P Paal and others, *Datenschutz-Grundverordnung: DS-GVO* (CHBeck 2017). Art. 9, Rn. 37.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

Chapter 6: Obligations of the data controller

The court, as a data controller responsible for the personal data processing performed by the court staff members constituting their work tasks, needs to have the internal structure and operations organized in compliance with the specific requirements of GDPR complemented by specific national legislation for personal data processing by the judiciary.[31] As the legislative process adopting or amending such specific national data protection legislation is at the time of finalization of this review yet to be concluded in a number of Member States, the assessment can be provided only with regard to general requirements emanating from GDPR itself.

Similar to all controllers, the data flows and operations representing processing of personal data should be documented and the documentation kept up to date in order to provide the court with usable overview of personal data processing landscape. Compared to commercial subjects, the internal organization of the court can be seen as rather rigid, with stable framework of operations and functions organized according to internal documents and plans based on legislative definition of the courts role as public judicial body. This stability allows for better assessment of most critical instances of personal data processing that should receive increased attention. These instances can be identified primarily based on criteria for personal data processing risk assessment,[32] which include e.g. size of the processed personal data evidence, relative sensitivity of the personal data, accessibility of the evidence, accuracy of the personal data, or forms of routine operations affecting the evidence. Notwithstanding the organizational specifics of each court, these instances can occur particularly in relation to log of the contents and manipulations with the court files, archiving of the court files, evidence of the correspondence, evidence of the presence at the court premises, database of the access authorization, or administration of the court information systems.

The assessment of necessary measures shall follow the risk-based approach; therefore the obligation is stricter for processing with higher level and probability of impact on rights and freedoms of natural

[31] Recital 20 GDPR.

[32] See e.g. scoring criteria for severity of personal data breach provided by ENISA. ENISA, 'Recommendations for a Methodology of the Assessment of Severity of Personal Data Breaches' (20 December 2013) <https://www.enisa.europa.eu/publications/dbn-severity> accessed 7 February 2018. p. 4.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

persons. On the other hand, the requirement of adequacy sets the upper threshold of compliance requirement and sets the boundaries on this regime of regulated self-regulation.[33]

6.1. Organizational obligations

The pursuit of adequate organizational measures cannot be seen as independent from the broader organizational framework of the court and its other requirements. As noted by Emery and De Santis; the proper setting of court management is a rather complex matter with many conflicting goals, functions and values.[34]

6.1.1. Responsibility of the data controller

From organizational perspective the measures required by personal data protection should include dutiful management of access authorization, proper chain of delegation within the court hierarchy with clearly defined roles and responsibilities, adequate or regular employee training and education, manuals and support in case of incidents or errors, internal audit and monitoring structures, cultivation of awareness to threats and security routines throughout the court work environment and further.

6.1.2. Record of processing activities

Many operations by the court staff are recorded or involve documentation of various personal data processing activities due to their established format in the court routine and requirements set by internal regulation or national legislation.

The applicability of the requirements set in Article 30 GDPR is bound to national approach to supervision of the personal data processing by the judiciary. As already mentioned above, the activities of court staff should be schematically documented and kept up-to-date in order to provide necessary input for adequate setting of organisational and technical measures. These records should, however, avoid granularity that would allow identification of particular cases, data subjects or activities, as such

[33] Paal and others (n 31). Art. 24, Rn. 3-4.
[34] Yves Emery and Lorenzo De Santis, 'What Kind of Justice Today? Expectations Of "Good Justice", Convergences And Divergences Between Managerial And Judicial Actors And How They Fit Within Management-Oriented Values' (2014) 6 International Journal for Court Administration:
<http://www.iacajournal.org/articles/abstract/10.18352/ijca.118/> accessed 28 January 2018.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

detailed documentation might present additional security risk as well as risk for the impartiality and independence of the court and the judge.

6.1.3. Security of processing

The matter of security requirements for personal data processing is closely linked to the general requirements on safety in the court environment. There are several foreign academic sources concerning the conceptual approach to the security and safety in court, particularly from the common law jurisdictions.[35] The general conclusion of these analyses may form a valuable base for further considerations of the adequate measures for secure personal data processing by the court staff. They do, however, severely lack adequate recognition of the modern challenges presented by court ICT technologies.

Security of processing presents particularly important narrow focused measures. Their adequacy is to be assessed relative to plausible threat scenarios. Such scenarios may take multitude of forms. In order to allow for their abstract classification, the personal data protection framework reflects the traditional concept of cybersecurity. The general aim of cybersecurity is to protect functions and functioning of the system. The common way to describe this goal is by the "CIA triad" of security objectives; (i) confidentiality, (ii) integrity and (iii) availability.[36] This classification is taken up by the Article 29 Working Party in guidelines on data breach notification[37] as well as by ENISA in recommendations for methodology of data breach assessment.[38]

The approach to security of processing should therefore go beyond the understanding of security in the court environment and reflect upon the importance of court systems as public information systems. Considered should be the risks related to breaches of confidentiality (e.g. access to data from personal

[35] See Michael Griebel and Todd S Phillips, 'Architectural Design for Security in Courthouse Facilities' (2001) 576 The Annals of the American Academy of Political and Social Science 118. or Anne Wallace, Deborah Blackman and Emma Rowden, 'Reconceptualising Security Strategies for Courts: Developing a Typology for Safer Court Environments' (2013) 5 International Journal for Court Administration <http://www.iacajournal.org/articles/abstract/10.18352/ijca.13/> accessed 28 January 2018.
[36] International Telecommunication Union, 'Definition of Cybersecurity' (*ITU*) <http://www.itu.int:80/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx> accessed 29 September 2017.
[37] Article 29 Data Protection Working Party, 'Guidelines on Personal Data Breach Notification under Regulation 2016/679 17/EN WP 250'. p. 6.
[38] ENISA (n 33).

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

insolvency registry, list of secret witnesses, expert witness documentation in sensitive cases), integrity (e.g. modification of the court file metadata, changes in dates, names, wrong attachment of files to cases, changes in operation logs) or availability (e.g. ransomware attack encrypting the court databases, DDoS attack on court electronic communication servers, deletion of electronic court files) of information sets including personal data. The appropriate measures and safeguards should follow the general recommendations and best practices for physical and cyber security as well as specific guidelines reflecting the particularities of the court system and sensitivity of the activities of the court staff.

6.1.4. Data protection impact assessment (DPIA)

It remains unclear to what degree should the court staff activities be subject to DPIA. Such assessment requirement may apply to the court as a whole, reflecting its capacity to process special categories of data on large scale as part of its main activities.[39] Similarly a particular DPIA may be necessary for the court information systems. Similar obligation should bind the provider of such a system; the court obligation should thereby be limited to modification of the general product DPIA for the particular setting of the court operations. With regard to other activities of the court staff, it seems unlikely that specific DPIA should be mandatory.

6.1.5. Relationship between court as the controller and data processors

Notwithstanding the low likelihood of variety of relationships between court as controller and third party as processor, it is a matter of the court as a whole or judiciary administration in general to arrange the necessary contractual framework for such relationships with regard to activities that may be performed and under which conditions. Such assessment is unlikely to have any specific features from the court staff perspective.

6.1.6. Supervision of the judiciary by data protection authority

The supervision of court activities within their judicial capacity through the DPA may present a challenge to the independence of the judiciary. Therefore a Member State may consider specific structure of supervision, which would transfer the role of DPA to a body within the judicial system to

[39] Article 35 para. 3 lit. b GDPR.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

avoid incursion into its independence. This presents a challenge for systems with imperfect separation of judiciary and partial administration through governmental executive body. This matter concerns the judiciary as a whole, the prism of court staff does not provide any specific aspects that should be taken into consideration.

The supervisory structure currently considered in the Czech Republic is based on the hierarchy of the judicial system. This is primarily because the Czech judicial system does not have a judicial council or other similar supreme administrative body for the judiciary. Thus the supervisory role shall be likely performed by court of higher instance towards corresponding courts of lower instance, with supreme courts having specific functional position created for supervisor of their compliance with data protection regulation. Due to the preservation of judicial independence and limitation of information that may be provided to data protection authority with regard to court files it is also likely that the data breach notification obligation shall be performed towards the corresponding court of higher instance.

In Bulgaria at the moment of finalization of this review, there is no public draft of legal act that will implement GDPR provisions into the national legislation. However, based on public speeches and interviews, it should be considered that the status-quo will be preserved and there will be one and only Data Protection Authority - the Commission for Personal Data Protection. Although the following statement should not be considered as definitive, most probably the Commission for Personal Data Protection will be the authority that should be notified in an event of data breach.

In Slovakia the aforementioned act No. 18/2018 Z. *z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov* (Act on personal data protection and on amendment and complementation of selected acts), stipulates that the supervisory role falls to the national DPA (*Úrad na ochranu osobných údajov Slovenskej republiky*) and this DPA shall be pursuant to § 40(1) of this act also notified by the courts about data breaches in accordance with GDPR obligations.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

6.2. Technical obligations

The continuously increasing ubiquity of dependence on ICT devices and their functions does not avoid the court environment. One side of the coin is the progress towards implementation of e-justice features in the judicial operations. Notwithstanding the diversity in current status of this development in various Member States, practically all courts have their court staffs operate with some form of information system, computer programs, internet connection and digital communication tools.[40] Already the connectivity of court systems processing data related to court files and other sensitive information presents a vulnerability that requires adequate cybersecurity response. Additional vulnerabilities may be added through more internal operations depending or being managed with the help of ICT systems (e.g. HR database of court staff, coordination and distribution of internal tasks, log of court files contents, operations with digitalized court files).

Further risk may originate from the use of personal devices by the court staff or other visitors to the court premises. Unintentional vulnerabilities may come from lenient wireless connection security policy at the court premises; consciously may these mobile devices be used for unauthorized record, duplication or circulation of internal documents containing sensitive personal data.

The significance of adequate cybersecurity measures is further underpinned by the eventual impact of court activities on high-stake situations. Even with omission of the criminal proceedings, the court may play crucial role in politically or personally highly sensitive matters.

The case files and other court documents tend to be accessed and processed by the court staff during their work tasks in their full-content version. The internal information systems and physical court files therefore allow relatively widespread and easy access to a broad spectrum of detailed personal data about clearly identified data subjects. Of particular sensitivity may be some forms of evidence, e.g. expert witness reports in medical malpractice cases (often including photographic documentation or intimate personal data related to personal health), evidence in cases related to financial compensation for victims of violent or sexual criminal offences, personal insolvency registry entries and files, reports, evidence and transcripts from divorce proceedings, adoption proceedings, paternity determination

[40] See European Commission for the Efficiency of Justice (n 21). p. 17-18.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

proceedings, evidence related to certain types of insurance claims, identity of protected witnesses in whistle-blower cases, witness statements and evidence in antidiscrimination or employment disputes, as well as cases related to other forms of infringement into personality rights.

The bulk of this information is in some instances and under certain constellation accessible to court staff assisting the judge at decision-making, managing the correspondence and court files, communicating with the witnesses and other stakeholders, searching and analysing the data available in the internal information systems and performing other task that are part of their respective role in the court internal structure.

The above described sensitivity of personal data processing operations within the court staff tasks necessitates considerations of threats related to internal (or external) intentional (or accidental) access, manipulation or erasure of case relevant information that include personal data. Such threats may have even elements of cyber warfare, if e.g. the court review of election results is taken into consideration.

If the court information systems are shared with other courts, indexed or in some other way include metadata structure for easier processing of the stored database of documents, this needs to be regarded as factors increasing the cybersecurity risks related to the processing of such personal data, as it increases the size of the database, simplifies the orientation and manipulation with its contents and opens new vectors for potential threat scenarios.

In response to these risks, the court is obliged to have adequate protective measures in place, mitigating the identified risks to acceptable level. Such requirements are similarly set in national cybersecurity legislation (currently under minimal harmonisation through implementation of Directive on security of network and information systems 2016/1148 and pursuant to guidelines and recommendations by European Union Agency for Network and Information Security (ENISA)). Aside from above mentioned organisational measures, it is particularly the technical checks and balances incorporated in the court information system, but also the physical premises of the court, that create the boundaries for secure processing of personal data during the court staff activities.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

6.2.1. Privacy by design

The newly articulated requirement of privacy by design is focused on appropriate incorporation of personal data protection considerations and measures from the onset of processing operations. Notwithstanding the respective relevance of principles relating to processing of personal data to all operations performed by the court staff, the rather rigid and stable setting of internal organisation of the court operations does present limited occasions necessitating the targeted application of the privacy by design requirement. A significant exception may be presented in case of modification of the work-flow routine, e.g. through adoption of new e-justice systems or innovative court file manipulation processes.

The related well established court practice is the court file access control. This also applies to the electronic case management systems that are present in in all Member States.[41] Strong regard to this requirement should be given by eventual introduction of electronic court file, as this systematic evolution may have profound impact on rights and freedoms of personal data subjects.

6.2.2. Privacy by default

The principle of data minimisation is an important maxim underlying the more specific requirements focused on securing of personal data processing. From a general perspective, the most secured personal data processing is such that never had to occur in the first place. The aim of privacy by default requirement is to strengthen this approach and limit the processing only to the necessary scope. However, such objective is to a certain degree conflicting with the role of court and fundamental maxims of its functioning. The objective of providing an effective remedy and court protection to all claiming their right in a dispute establishes more fundamental requirements of the court to be able to accommodate broad variety of tasks that involve collection, analysis and other forms of processing of various personal data with the aim of resolving the ensued dispute. Depending on the particular branch, form and instance of the court, this may require also active pursuit of evidence by the court or other activities that are rather focused towards gathering maximal amount of available information rather than its minimization.

[41] *Ibid.* p. 22.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

The requirement of privacy by default needs to be taken into consideration with respect to access authorisation and data storage, the particular legislative framework of procedural law and court organisation law is, however, to be likely reflected in the specific national data protection legislation. Privacy by default has more relevant application to e-justice systems, as there should be more detailed consideration taking place about the appropriate settings of data storage, access authorization, log management, administrator authority and other aspects, that need to reflect upon the principle of data minimisation.

6.3. Requirement of a data protection officer appointment

The matter of mandatory appointment of data protection officer (DPO) is better suited for the review of judiciary rather than the court staff. Nevertheless, to consider the regulatory framework, Art. 37 para. 1 lit. a excludes from the mandatory obligation courts acting in their judicial capacity. However, despite this exception, it must be considered, if the judicial capacity encompasses all activities of the court that represent personal data processing. Even if the aforementioned broad interpretation of the judicial capacity is applied, some auxiliary activities of the court staff may fall outside of this scope.

6.4. Reporting obligations

6.4.1. Reporting data breach to DPA

The personal data breach notification obligation is focused on impact mitigation. It is therefore a supplementary instrument to the security requirements under Article 32, which should include among other aspects also an effective detection of data breaches.[42] Despite available experience with a similar concept under certain national data protection laws or more broadly under the cybersecurity notification obligation for cybersecurity incidents, there remains uncertainty about application of these obligations to the judiciary. This is largely because the interpretation of the notification obligation under Article 33 is closely connected to the structure of supervision over the compliance by the judiciary. If the supervisory role is transferred to a specific body within the judiciary, the notification obligation should be towards this body. As such, particular communication platforms need to be

[42] Article 29 Data Protection Working Party, 'Guidelines on Personal Data Breach Notification' (n 38). p. 6.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

established between the general and specific DPA, in order to effectively share available information about occurring data breaches. At the same time, the specific structure of judiciary requires an increased focus on preventive measures, given that a data breach may indicate possible disruption of the court operations that may infringe upon e.g. the right to fair trial.

6.4.2. Notifying data breaches to affected data subjects

The communication of data breaches to the data subject in case of high risk to her or his rights and freedoms has an increased urgency with respect to his procedural rights and protection of fairness and justice of the trial. Adequate procedure should be put in place by the specific DPA body for judiciary, to be able to swiftly assess and respond to significant data breaches and provide affected parties with sufficient information and support to preserve their trust in the proper functioning of judicial system. Given the nature and complexity of modern day cyber threats, an occurrence of such data breach cannot be fully eliminated. It is therefore essential to implement adequate monitoring measures, reporting procedures and court staff training to minimize potential impact of such incident with timely response in organized and professional manner.

6.5. Awareness and guarantee of the rights of the data subject

The rights of the data subject are one of the core components of the personal data protection framework. GDPR aims for better balancing in the asymmetrical relationship between data controller and data subject, a proper possibility for exercise of these rights is therefore emphasized, particularly in Article 12. The data controller is given general obligation aimed at facilitating this, particularly through informing the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language and through sufficient cooperation. The requests by data subjects shall be processed in principle free of charge and without undue delay.

The primary right of the data subject pursuant to Articles 13 and 14 is the right to information about the basic aspects of the processing. This right is supplemented by right of access, which pursuant to Article 15 obliges the controller to provide the data subject per request information about the processing. In accordance with the principle of personal data accuracy, the data subject has a right to rectification of processed data (Article 16). Pursuant to maxim of data storage minimisation, the data

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

subject may under certain conditions expressed in Article 17 demand erasure of personal data concerning him or her. In cases of contested lawfulness of processing or accuracy of personal data, as well as in cases of legal interest in the data by data subject, he or she should be permitted to exercise in accordance with Article 18 the right to restriction of processing, which should lead to limited processing, but simultaneously preservation of the personal data concerned. If the data is processed by automated means based on consent, the data subject should be granted the right to data portability defined in Article 20. A broadly construed right to object pursuant to Article 21 obliges the data controller to demonstrate compelling legitimate grounds which override interests of the data subject for processing necessary for task under public interest or for legitimate interest of controller or third party. Data subject has also specific rights under Article 22 in case the processing has a form of solely automated individual decision making.

The exercise of these rights of data subject may, however, often be in conflict with the independence of judiciary and performance of judicial capacity by the court. For this purpose the Article 23 permits appropriate restriction of the rights and corresponding rights through national legislative measure. Such restriction must constitute necessary and proportionate measure in a democratic society to safeguard the protection of judicial independence and judicial proceedings and the enforcement of civil law claims. At the same time, the essence of fundamental rights and freedoms of the data subject must be respected. The rights to information pursuant to Articles 13 and 14 implement the principle of transparency, which can be applied to the processing by the court as a whole, rather than specifically to court staff operations. Right of access to processed personal data under Article 15 must be assessed with proportional balancing of the fundamental right of the data subject and potential risks to the independence of justice. Its performance towards auxiliary court staff activities is less likely to be restricted, if compared with processing related to court files. The right to rectification pursuant to Article 16 plays important role, if the erroneous or incomplete data could negatively affect the court proceeding. This right should the data subject be already able to routinely exercise with regard to mistakes in registries administered by the courts. The facilitation of the exercise of the right to object (Article 21) should be aligned with more general right to complaint, however, application of this right should not lead to obstacles in the court proceeding.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

Rights most likely to be restricted due to specific role of the judiciary are the right to erasure (Article 17) and right to restriction of processing (Article 18). Other rights, particular those related to data portability (Article 20) and right to human intervention in automated individual decision making pursuant to Article 22 para. 3, are not relevant to current form of judiciary arrangement.

The current discussion about restrictions to the rights of data subject pursuant to Article 23 with respect to Czech judiciary and court staff revolves mainly around application of safeguards for (d) the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security; (f) the protection of judicial independence and judicial proceedings; and (j) the enforcement of civil law claims. The draft of national law does not provide much further detail on the content in terms of judicial independence and judicial proceeding, the demarcation of judicial and non-judicial tasks of the court staff is therefore an open matter. Core of the judicial proceedings are activities handling the court case file, there are, however, numerous other court administrative agendas that also maintain court files, e.g. secretarial files, audit files, complaints files, foreign correspondence files. It is unclear, if the court should clearly classify all internal operations, or if such unambiguous sorting would be counterproductive and limit the internal flexibility needed for processing of various request by data subject that may aim towards obstructions in court proceeding.

The abuse of data subject rights under GDPR for procedural obstructions is an important topic. An associated issue is the formality of procedure for complaints and requests pursuant to Articles 12 to 23 GDPR. It is currently unclear, if the procedure shall be different for matters concerning judicial capacity of the court and matters outside such capacity. At this point, it seems that the procedure shall be informal and concluded by notice that does not constitute a formal decision in administrative proceeding. In such case, the effective remedy pursuant to Article 79 will most likely be provided by the administrative courts based on action for unlawful interference.

In Bulgaria there is at the moment of finalization of this review no legal act or draft of a legal act transposing GDPR into the Bulgarian legislation. It can therefore be only theorised on the nature

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

of the data subjects' request. Currently such a procedure falls under the scope of the formal administrative proceedings before the Commission for Personal Data Protection.

If the court as data controller violates the rights of the data subjects, they could benefit from the procedure outlined by the Act on Liability for Damages Incurred by the State and the Municipalities (ALDISM). The procedure under ALDISM is initiated before the competent administrative court.

The situation in Slovakia is at the moment also not yet clearly set. The current development tends to pursue similar direction as the one described above in case of the Czech republic.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

Chapter 7: Legal position of the data processor

As already described on previous instances in this review, from the perception of data processing by the court staff is the role of data processor rather secondary. The processing by court staff follows the regime of processing under the authority of the controller (or the processor) pursuant to Article 29.

The court in most cases takes up the role of the controller. The role of processor may be considered in instances of request from another court, the recipient court is, however, more likely to act as controller with regard to processing that it shall perform. The imperfect separation of state power between judiciary and executive branch in some Member States allow for additional set of situations, where the court may act as a processor instead of as a controller, e.g. if some aspects of the administration or management of the court (e.g. management of court premises, budgetary planning and accounting, central coordination of procurement) are performed by a governmental body (e.g. Ministry of Justice). It is, however, more likely that the court and the executive body will act as joint controllers.

The instances, where the court staff may act under the authority of the court as a processor, are therefore to be deemed as rare. Given the dependence of this setting upon the specifics of the national organisation of judiciary and particularities of the relationship between judicial and governmental bodies, it is not feasible to provide a general assessment of this setting with regards to the obligations of the court as a processor. Additionally, these obligations may be modified through the national legislation in order to preserve the functional independence of judiciary in accordance with Recital 20.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

Chapter 8: Administrative fines

The supervisory regime under GDPR introduces harmonized general conditions for imposing of administrative fines under Article 83 and 84. Given the specific position of the judiciary and the court staff the applicable rules are likely to be modified through specific national legislation. As already mentioned earlier in this review, it is likely that the supervisory role shall not be exercised by the data protection authority, but more likely through a specific judicial body or various courts. The liability for compliance with the data protection regulation by the court is to be held by the court statutory body, i.e. the court president, or as the case may be the chairman or magistrate. Despite the theoretical amount of applicable administrative fine for non-compliance, it is likely to presume, that these forms of sanctions shall function merely as motivation for court administration to ensure compliance, rather than applied instrument of its enforcement. Unduly formal pursuit of supervisory capacity over the court may otherwise interfere in judicial independence and effective functioning of the courts in their judicial capacity.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

Chapter 9: Relevant case law of CJEU and ECHR where court staff are involved

The analysis of relevant case law did not reveal any cases concerning particularly the position of court staff in the context of personal data processing. This may be given by several factors. Firstly, as presented in the first section, the concept of court staff is not unified and easily defined and as such presents a fragmented landscape without clear boundaries. Secondly, the legislative framework applicable to court organisation, functioning and internal operation is to a large degree specific for each Member State and outside the scope of EU legal framework. Third factor that may have contributed to the lack of relevant CJEU and ECHR case law is the role of court staff, which does not act as controller or processor with regard to personal data processing, but predominantly as employees, who act under the authority of the court or other controller or processor. As such, the employees are not directly liable for the non-compliance with the personal data protection legislation.

The broader consideration of court staff as employees of the court allows for consideration of their rights and freedoms with regard to personal data and privacy in this employment relationship. Security measures in court premises are likely to include camera surveillance, the work stations and employee devices may have monitored use of internet access, data transfer or initiated processes. CJEU emphasized in the decision of 28th October 2014 in the case C-582/14, *Breyer*, the frequent need for understanding of dynamic IP address monitoring as a form of personal data processing. In this light it is then highly relevant for court staff work stations monitoring the latest development in the ECHR case law in this context. The Grand Chamber of ECHR in its judgement of 5th September 2017 in the case *Bărbulescu v. Romania*, no. 61496/08, clarified the necessary conditions for compliance of employee monitoring with Article 8 of the European Convention on Human Rights, which provides a right to respect for one's "private and family life, his home and his correspondence". In the light of this case law, technical measures that may constitute a form of court staff monitoring need to be adequately designed with the aim of minimal effective intrusion, legitimate justification, proportionate consequences and sufficient notification of the monitored personnel in advance.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

Appendix

Fundamental principles relating to processing of personal data[43]

In Art. 5 of the GDPR the elementary principles for processing of personal data are determined in an abstract manner for the safeguarding of a high level of protection over the entire Regulation. Such a level of protection requires the application of the European Convention on Human Rights (hereinafter ECHR) requirements in terms of limiting "conditional"[44] fundamental rights, keeping in mind that, where the Charter of Fundamental Rights of the European Union (hereinafter EUCFR) does not offer a stronger protection than the ECHR, the meaning and scope of its provisions are the same of those of the latter[45]. As a result, the GDPR and the Police Directive ensure that each personal data processing act is legally based, pursues a legitimate aim, and is necessary and proportionate to the aim pursued.[46] In this way, the GDPR and the Police Directive standards constitute concretisations of the ECHR (including its Article 8 protecting the right to privacy), of the EUCFR (including its Article 8 protecting the right to personal data protection) and of Art. 16 para. 1 of the Treaty on the Functioning of the European Union (hereinafter TFEU).

In contrast to the former EU *Data Protection Directive*[47] (hereinafter DPD), the general principles of the *Regulation* are now directly applicable pursuant to Art. 288 para. 2 of the TFEU. With this change in the type of legislation comes noticeably an increased relevance of the following principles, since they are now binding in every scenario, where processing of personal data within the territorial and material

[43] This analysis was developed for the INFORM-project by Estelle De Marco (Inthemis, FR) and Matthias Eichfeld (University of Göttingen, DE).
[44] Some of the rights identified in the European Convention on Human rights are called "absolute", such as the right to life or to not be subjected to torture, while others are called "conditional" because they can be subjected to dispensations and/or limitations, as the right to respect for private life and the right to freedom of expression: Frédéric Sudre, 'La dimension internationale et européenne des libertés et droits fondamentaux', *in Libertés et droits fondamentaux*, under the direction of Rémy Cabrillac, Marie-Anne Frison-Roche, Thierry Revet, Dalloz, 11th ed., 2005, pp. 44-45.
[45] EU Charter of Fundamental Rights, article 52, 3.
[46] For further developments regarding the content of the notions of legal basis, legitimate aim, necessity and proportionality, see Estelle De Marco in Estelle de Marco et. al., Deliverable D2.2 – Identification and analysis of the legal and ethical framework, MANDOLA project (Monitoring and Detecting OnLine Hate Speech), GA n° JUST/2014/RRAC/AG/HATE/6652, version 2.2.4 of July 2017, Section 4.1.3, available at http://mandola-project.eu/publications/ (last accessed on 6 December 2017).
[47] Directive 95/46/EC.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

scope of the GDPR takes place.[48] In case of their violation claims for damages and sanctions may immediately follow.[49] Even though in numerous articles of the GDPR a certain concretisation of those principles takes place, it is mandatory to consider the fundamental determination in Art. 5 for each act of data processing.

1. Principles of lawfulness, fairness, transparency

Although the three principles standardised in Art. 5 para. 1 lit. a have reciprocal contexts in relation *to each other*[50]*, each notion has its own meaning.*

1.1. Lawfulness

A personal data processing constitutes a limitation of a fundamental right. As such, such limitation can only be legitimate if it first has a legal basis which must be clear, precise and predictable in its application[51]. This principle is recalled in the GDPR and in the Police Directive, as well as in Directive 95/46/EC. This principle means that the processing must be authorised by law. This law will be in most case the GDPR itself, where processing operations can fully comply with its provisions. But the GDPR provides for cases where an additional legal basis will be required, in order to, *inter alia*, provide for additional safeguards in particular contexts (for example in case of derogations to the provisions of Article 6 and of derogations allowed under Article 23). Where the GDPR constitutes a sufficient legal basis for a given data processing operation, the latter must in addition be based on the consent of the data subject or on any other legitimate basis provided for by law, as foreseen by both Art. 8 para. 2 of the EUCFR. and Article 6 of the GDPR, which provides more specifically for 6 possible legal foundations, including the data subject's consent and the legitimate interests pursued by the

[48] See *Heberlein*, in: Ehmann/Selmayr, Datenschutz-Grundverordnung, *C.H. Beck*, Munich 2017, Art. 5 para. 1; *Herbst*, in: Kühling/Buchner, Datenschutz-Grundverordnung, *C.H. Beck*, Munich 2017, Art. 5, para. 2; *Frenzel*, in: Paal/Pauly, Datenschutz-Grundverordnung, *C.H. Beck*, Munich 2017, Art. 5 para. 2.
[49] See Art. 82, para. 1 and Art. 83, para. 5 lit. a GDPR.
[50] See Judgement of the CJEU, 1 October 2015, C-201/14 (case "Smaranda Bara"), para. 32 et seq.
[51] See for instance Judgement of the CJEU, 20 May 2003, joined cases C-465/00, C-138/01 and C-139/01 (case "Österreichischer Rundfunk"); Judgement of the ECtHR, 4 December 2008, *Marper*, appl. n° 30562/02 and 30556/04.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

controller or by a third party. In order to use the latter legal basis a "test of legitimate interest" must be performed, and in this regards the Article 29 Working Party (becoming the European Data Protection Board in the GDPR)' and GDPR Recital 47 guidelines must be followed.

In addition, specific requirements from the rules governing the lawfulness of the consent[52] and processing of particularly sensitive data must be considered.[53] If there is a transfer of personal data to third countries or international organizations, the specific conditions in Chapter V of the GDPR must be taken into account.[54]

1.2. Fairness

The principle of fairness has been defined in Directive 95/46/EC as the prohibition of secrecy and the requirement of comprehensive information[55], and the meaning of the principle doesn't seem to have changed. The GDPR adds that, in particular, natural persons should be made aware of the existence of the processing, of the specific purposes for which personal data are processed and of risks, rules, safeguards and rights in relation to the processing of personal data and how to exercise their rights in relation to such processing, as well as of any further information necessary to ensure fairness such as the specific context and circumstances of the processing operations, and the question of whether personal data are mandatory and incurred consequences in case of silence.[56]

Furthermore, the principle of fairness has been seen by an author as an omnibus clause, which primarily covers situations in which the data subject experiences a disadvantage by processing their personal data, which is not in line with the overall picture of the balance of power between the data subject and the data controller, without necessarily violating a specific legal prohibition.[57] In other

[52] Art. 7 and 8 GDPR.
[53] Art. 9 and 10 GDPR.
[54] Art. 44 to Art. 50 GDPR.
[55] See Recital 38 to Directive 95/46/EC. See also Judgement of the CJEU, 1 October 2015, C-201/14 (case "Smaranda Bara"), para. 34.
[56] See Recital 39 p. 2 et. seq. and Recital 60.
[57] See *Herbst,* in: Kühling/Buchner, op. cit., Art. 5, para. 17; *Frenzel*, in: Paal/Pauly, op. cit., Art. 5 para. 20; *Kramer*, in: Auernhammer, DSGVO – BDSG, *Carl Heymanns Verlag*, Cologne 2017, Art. 5 para. 8-10.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

words, it enables to ensure transparency as a proportionality safeguard where an imbalance remains between the controller and the data subject, despite the respect of the other GDPR requirements.

1.3. Transparency

The principle of transparency adds, to the requirement of fairness or in other words of completeness of the information to be provided, a requirement of clarity of this information (it must be easily accessible, easy to understand, clear and in plain language)[58]. This principle applies to all the information that must be provided in order to ensure a fair and transparent processing.[59] The implementation as a new independent principle (that can be therefore seen as an extension of both the principle of fairness and the obligation of data subject's information) emphasises the importance of transparency as a fundamental proportionality safeguard, and therefore as a fundamental condition for the control over the use of one's own data and thus states a precondition for predictability and thereby effective protection.[60]

As a result, the principles of fairness and transparency concern together both the method and the content of the information.[61]

[58] See Recital 39 to GDPR.
[59] See Recital 58 p. 1 and Recital 39 p. 2. See also Art. 12 para. 1 GDPR.
[60] See Art. 29 Data Protection Working Party, Guidelines on transparency under Regulation 679/2016 (WP 260), p. 5, available at http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083 (last accessed 18 December 2017); see also Commission Staff Working Paper SEC (2012)72 final, Annex 2, Section. 2.4, available at http://ec.europa.eu/justice/data-protection/document/review2012/sec_2012_72_annexes_en.pdf (last accessed on 18 December 2017).
[61] See Art. 12 para. 1; Art. 13 para. 1 and Art. 14 para. 1; see also *Heberlein,* in: Ehmann/Selmayr, op. cit., Art. 5 para. 11.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

2. Principle of purpose limitation[62]

Art. 5 para. 1 lit. b GDPR stipulates that the collection of personal data is only permitted for specific, explicit, legitimate purpose and compatible use.[63]

2.1. Specified purpose

The requirement that the data may only be collected for specified purposes already follows directly from the wording of Article 8 para. 2 EUCFR and from the ECHR principle of necessity (which implies that the rights' limitation - i.e. the processing operations in our context - answers a specific important need -which must be precisely identified and justified-, in addition to be adapted to satisfy this need).

Each purpose must be *"sufficiently defined",* not later than the time of the data collection[64], *"to delimit the scope of the processing operation"* and therefore to enable the assessment of the data collection with the law and to enable the *"implementation of any necessary data protection safeguards"*.[65] This specification requires *"an internal assessment"* to identify and detail the kind of processing that *"is and is not included within the specified purpose"*.[66] This means that the controller must not gather data for possible future purposes that are not yet determined at the time of the collection and thus cannot be foreseen by the data subject.

[62] Some elements of the following discussion are coming from *Estelle de Marco* in: *Estelle de Marco* et. al., Deliverable D2.2 – Identification and analysis of the legal and ethical framework – MANDOLA project (Monitoring and Detecting OnLine Hate Speech), GA n° JUST/2014/RRAC/AG/HATE/6652, version 2.2.4 of July 2017, Section 4.2, p. 68 et seq.: The right to personal data protection, available at http://mandola-project.eu/publications/ (last accessed on 6 December 2017).
[63] Since these notions have already been part of the former DPD, the Article 29 Data Protection Working Party "Opinion 03/2013 on purpose limitation" serves as an adequate reference for further illustration of the principles, as far as no changes are indicated.
[64] See Recital 39 p. 6.
[65] Article 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation (WP 203), 2 April 2013, II.2.1, p. 12 and III.1.1, p. 15 et seq., available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf (last accessed on 6 December 2017).
[66] *Ibid.*, III.1.1, p. 15.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

Purposes too vague such as *"improving users' experience"* or *"IT-security purposes"* are usually not specific enough.[67] In the same line, an overall purpose to cover a number of separate purposes is not compliant.[68]

Only in certain situations, when a detailed description is clearly counter-productive because of its complexity, the specification or the purpose can be reduced to key information.[69] Nevertheless, a detailed description of the processing must be accessible via *"layered notice*" such as a link to a corresponding Internet page.[70]

In addition, since the principle of purpose specification is a practical application of the ECHR principle of necessity (of which weaknesses, in the framework of a complete necessity and proportionality tests, must be balanced by proportionality safeguards), it has to be noted that the performance of a necessity and of a proportionality tests can be used in order to find alternative safeguards that could satisfy data protection authorities and judges, in certain circumstances where the principle of purpose specification cannot be respected as written in the GDPR, such as certain kind of data collection performed in a Big data environment, using specific tools, some of the collected data being used as a second step for specific purposes, where the first motive of the collection can be found legitimate in itself even if too general (such as making profit of a EU based technology aimed at feeding innovative services while avoiding recourses to similar technologies produced in countries where the GDPR does not apply).

2.2. Explicit purpose

The purpose must be *"sufficiently unambiguous and clearly expressed"*[71], *"in such a way to as to be understood in the same way"* by the data controller and its staff including third parties processors, the supervisory authority and the data subjects.[72] This principle enables therefore all the parties *"to have a common understanding of how the data can be used"*, and reduces the risk to process data for a purpose that is not

[67] See for more examples *Ibid.*, III.1.1., p. 16.
[68] *Ibid.*, III.1.1, p. 16.
[69] *Ibid.*, III.1.1, p. 16.
[70] Article 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation, op. cit., III.1.1, p. 16.
[71] *Ibid.*, II.2.1, p. 12.
[72] *Ibid.*, III.1.2, p. 17.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

expected by the data subject.[73]In this way it enables data subjects to make informed choices.[74] The important thing is *"the quality and consistency of the information provided"*[75], in addition to its accessibility. Clearly there is a close relation between the explicit purpose and the principle of transparency and predictability, as these principles all aim to provide the data subject with complete information about the data processing (and at the end to ensure the proportionality of processing operations).[76] Especially for the accountability of the data processor, which Art. 5 para. 2, Art. 24 para. 1 and Art. 30 para. 1 lit. b GDPR require, the determination of an explicit purpose is mandatory.[77]

2.3. Legitimate purpose

As highlighted by the Article 29 Data Protection Working Party, *"the requirement of legitimacy means that the purposes must be in accordance with the law in the broadest sense. This includes all forms of written and common law, primary and secondary legislation, municipal decrees, judicial precedents, constitutional principles, fundamental rights, other legal principles, as well as jurisprudence, as such 'law' would be interpreted and taken into account by competent courts"*.[78]

2.4. Compatible use

The legal requirement of compatible use responds to the circumstance that it is technically possible to further process data for any purpose, once they have been collected and stored, and thereby interfering repeatedly in the right to protection of personal data. Pursuant to Art. 5 para. 1 lit. b further processing of the collected data is not permitted, if the manner of processing is not compliant with the purpose of the initial collection. It follows from the definition of 'processing' in Article 4 para. 2 GDPR that further processing includes not only the processing of the data for other purposes, but any processing

[73] *Ibid.*, III.1.2, p. 17.
[74] *Ibid.*, III.1.2, p. 17.
[75] *Ibid.*, III.1.2, p. 18.
[76] *Ibid.*, II.3, p. 13.
[77] See *Heberlein,* in: Ehmann/Selmayr, op. cit., Art. 5 para. 14.
[78] Article 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation, op. cit., III.1.1, p. 20.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

following the collection of the data, which therefore must be compliant with the initial act of collection.[79]

Since the conditions of all principles for the processing of personal data and the requirement of a legal basis for each processing must be fulfilled jointly[80], two cumulative conditions must be satisfied: further processing must not be incompatible with the purpose established during the collection of the data and there must be a sufficient legal basis for further processing.[81]

In this context, it is important to note that applying an anonymisation technique constitutes a further processing, which means that such an operation implies on the one hand that the personal data have been first collected in compliance with law, and on the other hand that such an anonymisation needs to be compliant with the fundamental principles (including the need for a legal basis) and the principle of compatible use.[82]

2.4.1. Meaning of recital 50 p. 2 in this context

This interpretation of Art. 5 para. 1 lit. b should also be maintained in the light of Recital 50 p. 2, which, according to its wording, gives the impression that there is no requirement for a separate legal basis in case of a compatible change of purpose. If that were the case, Article 5 para. 1 lit. b in combination with the wide criteria of Art. 6 para. 4 would have the character of a general clause-like extension of all legal bases of Article 6 para. 1.

Against such an understanding of the recital argues that the assessment of the purpose compatibility represents an additional limiting criterion, which was already established in similar terms in the former

---

[79] This notion of 'further processing' is also established in: Article 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation, op. cit., III.2.1, p. 21: "*any processing following collection, whether for the purposes initially specified or for any additional purposes, must be considered 'further processing' and must thus meet the requirement of compatibility*".

[80] See for the former DPD: Judgement of the CJEU, 1 October 2015, C-201/14 (case "Smaranda Bara"), para. 30 et seq.

[81] Article 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation, op. cit., III.2.1, p. 21; III.2.3., p. 33; See furthermore Article 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation, op. cit., II.2.1, p. 12, fn. 28: "*Article 8 (2) of the Charter also makes it clear that the requirement of purpose specification is a separate, cumulative requirement that applies in addition to the requirement of an appropriate legal ground.*"; See also *Heberlein,* in: Ehmann/Selmayr, op. cit., Art. 5 para. 19; *Herbst,* in: Kühling/Buchner, op. cit., Art. 5, para. 42.

[82] Art. 29 Data Protection Working Party, Opinion 05/2014 on Anonymization Techniques (WP 216), 10 April 2014, 2.2.1, p. 7, available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf (last accessed on 6 December 2017).

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

DPD.[83] Since there is no indication in the GDPR except for the wording in recital 50 p. 2 for such a new understanding of the principle of compatible use, the wording can only be understood as meaning that no new legal basis is required if the subsequent processing involves the execution of the initial processing and meets the conditions of the legal basis for the initial processing. A different interpretation of recital 50 p. 2 would be incompatible with the principle of lawfulness of Art. 5 para. 1 lit. a and the overall protective purpose of the GDPR, which is stated in Art. 1 para. 2.[84]

2.4.2. Key factors for purpose compatibility assessment

For further processing, in addition to the existence of a new corresponding legal basis, a detailed examination of the compatibility of the purposes has to be carried out. According to Art. 6 para. 4, the test is mandatory where "the processing for a purpose other than that for which the personal data have been collected is not based on the data subjects consent or on a Union or Member State law[85]".

This determination is followed by a non-exhaustive list of criteria for such a process, which is essentially based on the factors developed by the Art. 29 Data Protection Working Party.[86]

- *Any link between the purposes for which the data have been collected and the purposes of further processing, Art. 6 para. 4 lit. a:*

  The issue is to analyse the 'substance' of this relationship, to notably determine if the further processing was "*already more or less implied in the initial purposes, or assumed as a logical next step in the*

[83] Following the rapporteur of the EU-Parliament involved in the trilogue negotiations *Jan Philipp Albrecht*: *Albrecht*, Das neue EU-Datenschutzrecht – von der Richtlinie zu Verordnung, Überblick und Hintergründe zum finalen Text für die Datenschutz-Grundverordnung der EU nach der Einigung im Trilog, in: Computer und Recht 2016, 88 (92); See furthermore the assessment of state council and desk officer of the German Ministry of Justice and Consumer Protection *Peter Schantz*: *Schantz*, Die neue Datenschutz-Grundverordnung – Beginn einer neuen Zeitrechnung im Datenschutzrecht, in: Neue Juristische Wochenschrift 2016, 1841 (1844); See also *Herbst,* in: Kühling/Buchner, op. cit., Art. 5, para. 49; *Buchner/Petri* in: Kühling/Buchner, op. cit., Art. 6, para. 182 et seq.; *Heberlein,* in: Ehmann/Selmayr, op. cit., Art. 5 para. 20.
[84] See *Heberlein,* in: Ehmann/Selmayr, op. cit., Art. 5 para. 20; *Herbst,* in: Kühling/Buchner, op. cit., Art. 5, para. 49.
[85] Such a law must protect the important public interests referred to in Article 23 para. 1 of the GDPR, the data subject or the rights and freedoms of other persons and must comply with the proportionality test required by Article 52 para. 1 of the EUCFR and Article 8 of the ECHR. See Judgement of the CJEU, 6 October 2015, C-362/14 (case "Schrems"); Judgement of the CJEU, 8 August 2014, C-293/12 (case "Digital Rights Ireland").
[86] Article 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation, op. cit., III.2.1, p. 21; III.2.2, p. 23 et seq.; The GDPR lists five principles but two of them are handled under the same one by the Article 29 Data Protection Working Party.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

processing according to those purposes", or if there is only a "*partial or even non-existent link with the original purposes*".[87]

Although the compatibility requirement is usually missing between the processing for a purpose of a contract and the notice of potential criminal offenses or any potential public security threat given by the data controller to the competent authorities, in such a case there is a legitimate interest of the data controller (Art. 6 para. 1 lit. f) for the display and transmission of personal data.[88] Of course, this does not apply if the data controller is subject to a confidentiality obligation.[89]

- *The context in which the data have been collected, Art. 6 para. 4 lit. b:*

  This assessment should be based, above all, on the 'reasonable expectations' of the data subject resulting from the relationship with the data controller.[90] The more surprising and unpredictable further processing is for the data subject, the more indicates to an incompatibility with the original purpose.[91] For instance, it is incompatible to use security monitoring to control workers, a breathalyser to check working hours or to collect fingerprints of asylum seekers for the initial purpose of prevention from filling multiple asylum applications in different member states simultaneously but using them for law enforcement purposes later on.[92]

- *The nature of the personal data, Art. 6 para. 4:*

  This criterion refers especially to the further processing of special categories of personal data (Art. 9) or personal data related to criminal convictions and offences (Art. 10), but also communication data, location data or whether the data subject is a child or belongs to a more vulnerable segment of the population requiring special protection.[93] As a result, a particularly

[87] Article 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation, op. cit., III.2.2, p. 23 et seq.
[88] Recital 50 p. 9.
[89] Recital 50 p. 10.
[90] Recital 50 p. 6.
[91] Article 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation, op. cit., III.2.2, p. 24.
[92] Article 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation, op. cit., Annex 4, p. 56 et seq., 68.
[93] Article 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation, op. cit., III.2.2, p. 25, fn. 68.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

careful examination is necessary.[94] As well, the general principles and the special requirements for the protection of sensitive data must be considered in such a further processing.[95]

- *The possible consequences of the intended further processing for the data subject, Art. 6 para. 1 lit. d:*
  Both positive and negative consequences must be taken into account for the assessment.[96] According to the risk-based approach of the GDPR (Art. 24 para. 1), potential risks must be included such as the publication of the data or other making accessible to a larger group of people, the processing by third parties or whether a combination with other data takes place.[97] This applies especially if there is a risk of discrimination or damage to the reputation of the data subject.[98]

- *The existence of appropriate safeguards, Art. 6 para. 4 lit. e:*
  Such as in a proportionality test, appropriate safeguards need to be implemented in order to ensure both (1) that the freedoms' limitation will not be higher than the one that has been assessed (through ensuring that the context, conditions and content of the intended processing will not be modified - including protection mechanisms already implemented), and (2) that weaknesses identified during first steps of the compatibility test and compensated. These safeguards may consist in the first place in technical and/or organisational safeguards ensuring *inter alia* anonymisation each time this is possible[99] or "functional separation", which includes the consideration of, encryption and pseudonymisation[100] techniques and of aggregation techniques[101], in other words the consideration of measures ensuring that the "*data cannot be used to take decisions or other actions with respect to individuals*"[102]). These safeguards may also consist

[94] *Ibid.*
[95] Recital 50 p. 8.
[96] Article 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation, op. cit., III.2.2, p. 25.
[97] *Ibid.*,
[98] Recital 75.
[99] See for example Recital 39 of the GDPR; Article 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation, op. cit., III.2.2, p. 27
[100] See the Definition in Art. 4 No. 5.
[101] Article 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation, op. cit., III.2.2, p. 27.
[102] *Ibid.*

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

in ensuring transparency (including purpose re-specification) and data subjects' control (collection of users' new consent, opt-out possibilities, data subjects' rights…)[103].

2.4.3. Compatible use in case of privileged purposes

According to Art. 5 para. 1 lit. b archiving purposes, scientific or historical research purposes or statistical purposes are considered as privileged purposes, which means that there is a presumption of conformity for such a purpose. However, the lawfulness of the further processing for these purposes presupposes that it complies with the conditions laid down in Article 89 para. 1. The latter provides for appropriate guarantees for this process which may be supplemented and specified in the form of member state legislation.[104] Amongst those guarantees, lies the requirement to perform a compatibility test in order to identify all safeguards that are appropriate to the specific context[105]. Besides, any such processing must of course also comply with all the fundamental principles of Art. 5[106] and more generally with all the other requirements of the GDPR, including the requirement to be based on one of the grounds listed in Article 6 para 1 of the GDPR[107] and the requirement to inform the data subject of the processing' purposes and of his or her rights.[108]

[103] *Ibid.*
[104] Art. 89 para. 2 and 3.
[105] This requirement has been highlighted by the Article 29 Data Protection Working Party (Opinion 03/2013 on purpose limitation, *op. cit.* III.2.3, p.28) in relation to Article 5 of Directive 95/46/EC. However, it is also applicable in the context of the GDPR since its Article 5 refers to Article 89, which requires the implementation of "safeguards (that must be) "*appropriate (...), in accordance with this Regulation*" (while the Directive required the provision of appropriate safeguards). Safeguards proposed in Article 89 of the GDPR are only elements of a proposed list that must be complemented by all the safeguards that are appropriate in the specific context.
[106] Recital 50 p. 8.
[107] Article 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation, *op. cit.*, III.2.3, p.28. This opinion has been delivered in relation to Article 6b of Directive 95/46/EC. However, the formulation of Article 5 of the GDPR being almost the same, this decision appears to be applicable in this context too.
[108] Recital 50 p. 8.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

3. Principle of data minimisation

Art. 5 para. 1 lit. c states that the processed data must be "*adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed*". According to this principle, personal data may only be processed if the purpose of the processing cannot be reasonably achieved by other means.[109] This includes the implementation of anonymisation techniques if possible, which would cease the personal reference and thus the data would be no longer subject to data protection law.[110] Obviously, there is a close relation to the principle of time limitation for data storage.

A specification of this principle takes place, inter alia, in the concepts of privacy by design and by default in Art. 25.

[109] Recital 39 p. 9.

[110] See *Herbst,* in: Kühling/Buchner, op. cit., Art. 5, para. 58; See for the procedure of anonymisation: Art. 29 Data Protection Working Party, Opinion 05/2014 on Anonymization Techniques, op. cit., 2.2.1, p. 7 et seq.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

4. Principle of accuracy

According to Art. 5 para. 1 lit. d personal data must be "*accurate and, where necessary, kept up to date*". To ensure the data quality, the data controller must actively take every "*reasonable step*" to rectify or delete inaccurate data without delay.[111] Since the usage of personal data might produce legal consequences for the data subject, the data shall reflect reality at any given time.[112]

To enforce this principle, the data subject has the right to rectification (Art. 16) and the right to erasure (Art. 17).

It is important to notice that this obligation must be complied especially with respect to the purposes and the specific circumstances of processing.[113] For instance, if the processing purpose is preservation of evidence it can be necessary to process outdated data.[114]

[111] Art. 5 para. 1 lit. d; Recital 39 p. 11.
[112] See *Voigt/von dem Bussche*, in: Voigt/von dem Bussche, The EU General Data Protection Regulation (GDPR) – A Practical Guide, *Springer*, Cham (Switzerland) 2017, 4.1.4, p. 91; *Frenzel*, in: Paal/Pauly, op. cit., Art. 5 para. 39.
[113] Art. 5 para. 1 lit. d.
[114] See *Heberlein,* in: Ehmann/Selmayr, op. cit., Art. 5 para. 24; *Frenzel*, in: Paal/Pauly, op. cit. Art. 5 para. 40 et seq.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

5. Principle of storage time limitation

Art. 5 para. 1 lit. e determines that the storage period of personal data should be kept to a 'strict minimum'.[115] Decisive for the permissible duration of storage is the purpose of the processing. Thus, the principle of storage time limitation is an application of the principle of proportionality defined in terms of time. In order to preserve this principle, it is sufficient to remove the personal reference of the data (identifiability) according to the wording in Art. 5 para. 1 lit. e.[116]

To ensure the concept of limitation the data controller should establish time limits for erasure and for a periodic review.[117] Pursuant to Art. 13 para. 2 lit. a, Art. 14 para. 2 lit. a and Art. 15 para. 1 lit. d the data controller must inform the data subject of the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period.

To enforce this principle, the data controller is obliged to erase personal data under the provision of Art. 17.

Similar to the constitution of privileged purposes in Art. 5 para. 1 lit. b, there are exceptions to the principle of storage time limitation as well. If the personal data is processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, the storage for a longer period is explicitly allowed.[118] In such a case, appropriate guarantees in accordance with Art. 89 para. 1 are required.

[115] Recital 39 p. 8.
[116] See Recital 26 p. 3 and 4 for further explanations on the criterion of identifiability.
[117] Recital 39 p. 10.
[118] Art. 5 para. 1 lit. e.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

6. Principle of integrity and confidentiality

According to Art. 5 para. 1 lit. f processing must be carried out "*in a manner that ensures adequate security of personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures*".[119]

In this way, the principle addresses the need for organisational safeguards for the processing operation. Specifications of the protective measures especially take place in Art. 32, Art. 28 para. 2 p. 2 lit. b and Art. 29.[120] Moreover, personal data breaches must be reported to the supervisory authority (Art. 33) and, in certain situations, to the data subject (Art. 34).

[119] See also recital 39 p. 12.
[120] For further explanations to the concrete nature and extent of adequate protective measures see the sections of the specific obligations of data controller and data processor.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

7. Accountability

The data controller is responsible for and must be able to **demonstrate compliance with the fundamental principles** relating to processing of personal data, Art. 5 para. 2.[121] The extended obligation of accountability is an expression of the enhanced self-responsibility of the data controller under the GDPR.

7.1. Liability of the data controller or data processor

Irrespective of the possibilities of the data subject for remedy against the processing activity of the data controller (Art. 77-79), any infringement of the regulation may lead to a claim for compensation of damage caused by processing, unless the controller or the processor has complied with the obligations of the regulation, Art. 82.

7.2. Accountability and data protection by design and by default[122]

A specification of the notion of self-responsibility takes place in Art. 24 which requires of the data controller to "*implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with*" the regulation, "*taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons*". As recital 75 phrase 2 points out, this can be done by having the data controller adopt internal strategies and take measures that comply with the principles of data protection by design and by default (Art. 25 para. 1 and 2).

In any case the data controller must ensure accountability by keeping a record of processing activities (Art. 30), cooperating with supervisory authorities (Art. 31), reporting and notification of data breaches

[121] See for the notion also Article 29 Data Protection Working Party, Opinion 03/2010 on the principle of accountability (WP 173), 13 July 2010, III.2, p. 9 et. seq., available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2010/wp173_en.pdf (last accessed on 15 December 2017).
[122] For further explanations on the concept of accountability see the sections of the specific obligations of data controller and data processor.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

(Art. 33, 34), carrying out a data protection impact assessment in certain situations (Art. 35) and the corresponding prior consultation of the supervisory authority (Art. 36).

The overall responsibility and accountability of the data controller include the responsibility for the processing of the data processor (who is acting on behalf of the data controller).[123] Nevertheless, the processor is also demanded to take appropriate technical and organisational measures to take care of the risk associated with data processing.[124]

[123] Art. 28 para. 1.
[124] Art. 32 para. 1.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

8. Prohibition of automated decision-making

Not in Art. 5 but in Art. 22 of the GDPR the right of the data subject is stated, "*not to be subject to a decision solely based on automated processing, including profiling, which produces legal affects concerning him or her or similarly significantly affects him or her*". From the perspective of the data controller, this determination leads in turn to the fact that there is a prohibition on fully automated decision-making that has a legal or similarly significant effect concerning the data subject.[125] A decision is based solely on automated processing if there is no human involvement and the outcome of the processing is not reviewed by a competent and authorised person.[126] The intention is that the data subject shall have the right to a final decision by a human being if the decision implies an increased risk for his or her situation.[127]
The wording of Art. 22 para. 1 and the complementary recital 71 indicate a narrow interpretation of 'similarly significant effects', since it is in a close context to 'legal affects'. According to the Art. 29 Data Protection Working Party it depends upon the characteristics of each case, including:

- the intrusiveness of the profiling process;
- the expectations and wishes of the individuals concerned;
- the way the advert is delivered; or
- the particular vulnerabilities of the data subject targeted.[128]

As a result, certain practices of targeted online advertising may have such an effect, especially when it comes to differential pricing strategies.[129]

There are three exceptions to the prohibition listed in para. 2 of Art. 22: If the automated-decision making is necessary for the performance of a contract between data controller and data subject, if there

[125] See Art. 29 Data Protection Working Party, Guidelines on automated individual decision-making and Profiling for the purposes of Regulation 679/2016 (WP 251), 3 October 2017, II., p. 9, available at http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083 (last accessed 18 December 2017).
[126] *Ibid.*, II.A., p. 9 et seq.; See also *Schrey*, in: Rücker/Kugler, New European General Data Protection Regulation – A Practitioner's Guide, *Nomos, C.H. Beck, Hart*, Baden-Baden, Munich and Oxford 2017, p. 149, para. 692.
[127] See Art. 29 Data Protection Working Party, Guidelines on automated individual decision-making and Profiling for the purposes of Regulation 679/2016., op.cit., II.B., p. 10 et seq.
[128] *Ibid.*, II.B., p. 11.
[129] *Ibid.*

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

is an authorisation provided by Union or Member State law or if the data subject has given his or her explicit consent. Regarding special categories of data (Art. 9 para. 1) the exceptions for automated decision-making are not applicable, unless the conditions of Art. 9 para. 2 lit. a or g are met. In all cases, it is necessary to "*implement suitable measures to safeguard data subject's rights and freedoms and legitimate interests*"[130].

[130] Art. 22 para. 2 lit. b, para. 3, para. 4.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.