SOTER

# Training Handbook: **ONBOARDING**

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833923

Authors: Miren Karmele García García, Eliseo Venegas Mayoral and Nora Schreier
Design and Layout: Matthew Reilly and Ekaterina Kyulyumova



Published in January 2022 (Graz/Dublin/Madrid)

ISBN: 978-3-903374-11-9
DOI: 10.25364/978-3-903374-11-9

# Table of contents

# SOTER Training Handbooks Introduction

The financial sector is experiencing a real digital revolution in recent years, in which traditional entities are becoming providers of digital services in order to remain competitive. Although it is clear that this new era implies many advantages for businesses and citizens, in addition, the release of new digital services and connections imply the appearance of new threats and risks in terms of cybersecurity, data privacy and the use of digital identities.

These threats must be tackled under a holistic approach and pointing at their different origins, including the human factor.

Furthermore, the current regulations to be met, apart from involving a technological and mind-set challenge and increasing the number of entities with which to interact with, also aim to create or improve tools to prevent fraud and reduce cyber vulnerabilities as much as possible.

SOTER takes the challenge, considering both technological and non-technological (human factor and governance within organizations) aspects and providing innovative solutions that will act as a transformative process of the finance sector, helping their players to increase their cybersecurity level, improving the fight against present and future cyber attacks and vulnerabilities and, to summarise, increasing their cyber-resilience.

SOTER tackles two main challenges: how to improve the process of digital onboarding and how to implement state of the art cybersecurity culture.

**This handbook summarizes the outcomes on the SOTER work on digital onboarding.**

# 1

# Digital Identity and Digital Onboarding

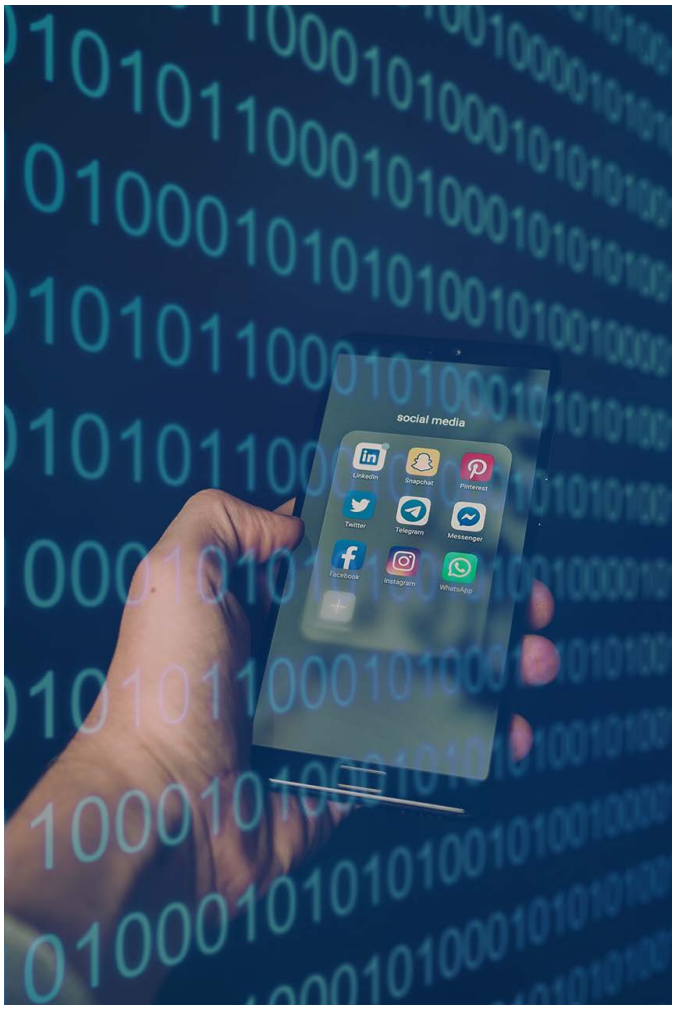
Identity verification and authentication are two processes at the heart of many of our daily digital interactions – from providing our password on our mobile phones to logging into our email or social media account.

In the finance sector identity verification and authentication are two of the most important factors in maintaining a safe and secure banking environment.

The finance sector is changing at a rapid pace, with many of the existing services moving to digital only platforms, whilst novel new services and technologies appear for the 21st century banking customer.

Know Your Customer services are a key component of ensuring that financial services are kept secure, as service providers seek to ensure they know the person that is engaging with the financial system.

At the heart of SOTER's solution is the concept of Digital Identity. The goal is to provide the banking client with a verifiable digital identity, streamlining the process of engaging with new finance service providers, as they are able to reuse the same proof of their identity for many service providers.



# SOTER Digital Onboarding Platform

One of SOTER's main results is the Digital Onboarding Platform, which is a technological tool to facilitate the interconnections between different services providers and the users in a simple way.

It has been developed to provide identification and onboarding to allow the delivery of electronic transactions at any time, in a transparent way, to any kind of service provider belonging to any market sector in an independent way. This approach allows the end-user entity to focus on their core business and to detach itself from investing on creating such identification services compliant with regulations because SOTER platform will provide this ready for them.

## 2.1. Digital Onboarding Platform services

The Digital Onboarding Platform is the combination of different biometric, e-signature and security services that make up a complete and scalable digital onboarding solution.

### IDENTIFICATION SERVICES

Services that allow highly secure identification of customers remotely

### ELECTRONIC SIGNATURE SERVICES

Electronic signature services that, relying on trusted European service providers, allow customers to sign contractual documents remotely

### ANTI-FRAUD SERVICES

Services to generate a unique fingerprint of customer devices in order to detect and prevent fraudulent behavior

### GLOBAL CONSENT MANAGEMENT SERVICES

Services enabling the global management of customer consents in the financial institution

### DATA PROTECTION & MANAGEMENT SERVICES

Services that allow the management and safekeeping of data and evidence captured in the process for the required number of years

### SUPPORT PORTALS

Portals integrated with Salesforce and CAD for managing onboarding processes by back-office agents

## 2.2. Digital Onboarding Platform benefits vs Traditional processes

The digital onboarding platform is a highly flexible & configurable platform that enhances the user experience and adapts to future market needs. All this while applying the highest security measures in the industry.

**COMPLETE ONBOARDING**

100% complete onboarding process, from video-identification to the signing of the contract documentation

**MODULAR SOLUTIONS**

The possibility to construct different customer journeys

**IMPROVED USER EXPERIENCE**

By capturing identification data via NFC vs. OCR, we do not depend on the quality of the camera or the lighting of the environment

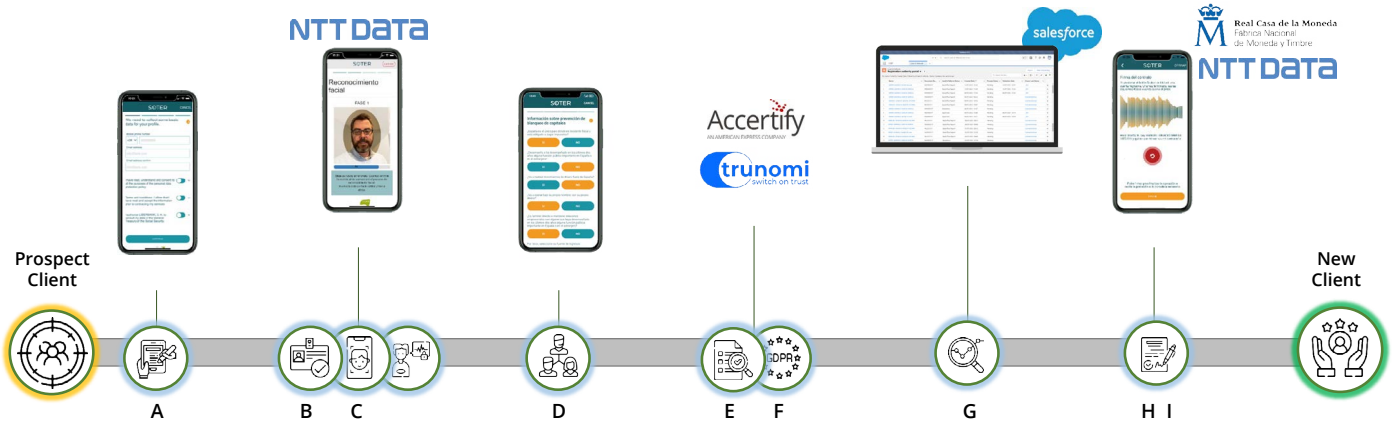
**INNOVATION LABORATORY & COMPLIANCE ADAPTABILITY**

Integration of third-party solutions in an agile and cost-effective way

**MAXIMUM SECURITY**

Robust solutions implemented in high security environments such as police and airports

## 2.3. Digital Onboarding Platform example




### A: Basic customer data intorduction

- Mobile phone
- Mail
- Consents
- Precontractual information

### B: Videoidentification:

- Document data capture via NFC
- Facial biometric validation
- Proof of life

### C: Voice biometric pattern:

- User voiceprint capture

### D: Know Your customer

Socio-economic:

- Social security
- Occupation
- Public charges
- ets

### E: Accertify- InMobile:

- Device's unique
- PermID generation
- Execution of rules associated to the device

### F: Trunomi

- Global management of consents
- Digital notary

### G: Registration authority portal:

- A certified backoffice agent validates that the data is correct
- Onboarding process metrics

### H: Contract signature:

- Contracts are signedusing the user's biometric voice pattern.

### I: Evicence custody:

- Custody of all evidence of the onboarding process for a defined period of time

# 3

# Threats and Risks

The European Commission presents in its report on remote onboarding solutions in the banking sector[1] some of the most important risks in digital onboarding platforms. These are the risks associated with identity fraud:

- **1st party claimed impersonation**: The account holder claims to have been impersonated, when in fact they opened the account.
- **1st party partial identity fraud:** The prospective customer falsifies an element of their identity to open the account which would otherwise be refused, e.g., date of birth or address history.
- **1st party friendly impersonation**: Family member accurately impersonates another family member.
- **1st party collusion:** Applicant opens the account for the purpose of providing login credentials and payment instruments to another person who will permissively adopt the identity of the account holder.
- **Identity theft:** Third party impersonates another person. Forged and altered identity documents to match the identity information and physical features of the fraudster aimed at defeating biometric comparison.
- **Deceased impersonation:** The fraudster impersonates the identity of a deceased person.
- **False identity:** Creation of a false persona supported with synthetic proofs of identity.
- **Legal entity identity theft:** Changing information held in public registers of corporate ownership, officers, address, to correlate the whereabouts of the legal entity to false identities and physical locations under the control of fraudsters.

Another risk to be taken into account in onboarding platforms are software vulnerabilities. Software vulnerabilities are defects in the code that can cause catastrophic consequences to the confidentiality, integrity or availability of data and services in the Onboarding process. These defects can cause unintentional breaches of security or can be exploited by attackers to damage the Onboarding process, compromising the availability of the process, or obtaining some benefits by stealing or modifying data.

**Most critical risks**

The most critical risks identified in onboarding platforms, and the ones that always must be adressed are the following:

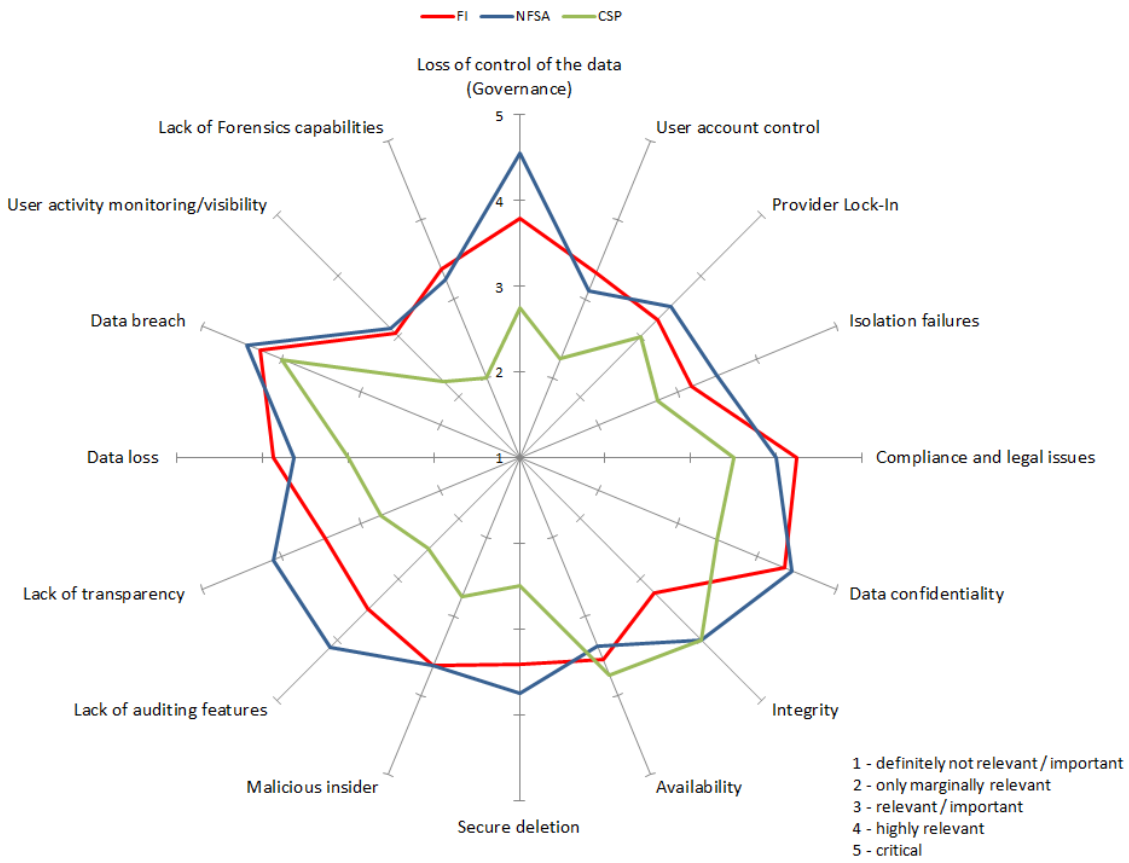
- Abuse of access privileges
- Insecure interfaces and APIs
- Insecure or ineffective deletion of data
- Malware diffusion
- Social engineering
- Software vulnerabilities
- Deliberate alteration of information
- Denial of service

**Risks related to cloud based services**

ENISA[2] conducted a survey of cloud service providers (CSPs), National Financial Supervisory Authorities (NFSAs) and Financial Institutions (FIs), asking respondents to rank a list of common security risks on a scale of one to five (five being the greatest concern). The graph shows the results of this survey.

1 https://ec.europa.eu/info/sites/default/files/business_economy_euro/banking_and_finance/documents/report-on-existing-remote-on-boarding-solutions-in-the-banking-sector-december2019_en.pdf

2 https://www.enisa.europa.eu/publications/cloud-in-finance




This research has led to the conclusion that one of the most common attacks in the cloud are malware injection attacks. An example of this occurred in 2008, when Sony's PlayStation website was the victim of a SQL injection attack.[3]

Another attack to be aware of is the denial-of-service attack. They are designed to overload a system and make services unavailable to its users. An example of this type of attack occurred when security experts Bryan and Anderson organised a denial-of-service attack exploiting the capabilities of Amazon's EC2 cloud infrastructure in 2010. As a result, they managed to make their client unavailable on the Internet by spending only $6 on virtual service rentals.

There are also known examples of account or service hijacking attacks, one of which is when an employee of Salesforce, a SaaS provider, was the victim of a phishing scam that led to the exposure of all of the company's customer accounts in 2007. This type of attack occurs when accounts or services are hijacked after gaining access to a user's credentials.

Man-in-the-cloud attacks must also be taken into account, in this type of attack, hackers intercept and reconfigure cloud services by exploiting vulnerabilities in the synchronisation token system so that, during the next cloud synchronisation, the synchronisation token is replaced by a new one that gives the attackers access. In addition, there are two new cyber-attacks called Spectre and Meltdown, which appeared earlier this year and have already become a new threat to cloud computing. With the help of malicious JavaScript code, adversaries can read encrypted data from memory by exploiting a design weakness in most modern processors. Both Spectre and Meltdown break the isolation between applications and the operating system, allowing attackers to read information from the kernel.

3 https://www.apriorit.com/dev-blog/523-cloud-computing-cyber-attacks

# 4

# Risk Mitigation

## 4.1. How to mitigate identified risks

Base on previous Risk Assessment done to the SOTER platform, the most relevant security measures to mitigate risks on the onboarding platform and other similar ones are presented:

- **Vulnerability scanning:** Systematic examination of SOTER components and products is necessary to determine the adequacy of security measures, to identify security weaknesses, to provide data from which to predict the effectiveness of proposed security measures, and to confirm the adequacy of such measures after implementation.
- **Penetration testing:** Penetration testing is a specialised type of assessment conducted on information systems or individual system components to identify vulnerabilities that could be exploited by adversaries.
- **Remote access:** The organisation establishes and documents usage restrictions, configuration/connection requirements and implementation guidelines for each type of remote access allowed; and authorises remote access to the information system before allowing such connections.
- **Contingency planning:** The organisation coordinates the development of the contingency plan with the organisational elements responsible for related plans.
- **Fault remediation:** Organisations identify, report and correct information system failures, test all new software and firmware upgrades prior to installation, and incorporate fault remediation into the configuration management process.
- **Denial-of-service protection:** A variety of technologies exist to limit, or in some cases, eliminate the effects of denial-of-service attacks.

## 4.2. Security related to third-party relationships

It recommends measures to be applied in the PDO and relevant to the relationship with third parties and their systems.

- **Third-Party Personnel Security:** The organisation establishes personnel security requirements including security roles and responsibilities for third-party providers; requires third-party providers to comply with personnel security policies and procedures established by the organisation; and to notify of any personnel transfers or terminations of third-party personnel who possess organisational credentials and/or badges, or who have information system privileges.
- **Trusted Path:** The information system provides a trusted communications path that is logically isolated and distinguishable from other paths.
- **Application Partitioning:** The information system prevents the presentation of information system management-related functionality at an interface for non-privileged users.
- **External Information System Services:** The organisation will require that providers of external information system services comply with organisational information security requirements and employ in accordance with applicable federal laws, executive orders, directives, policies, regulations, standards, and guidance; Defines and documents government oversight and user roles and responsibilities with regard to external information system services; and, employs techniques to monitor security control compliance by external service providers on an ongoing basis.
- **System Interconnections:** Organisations can constrain information system connectivity to external domains by employing one of two policies with regard to such connectivity: allow-all, deny-by-exception (also known as blacklisting or deny-all), allow by exception (also known as whitelisting).
- **Use Of External Information Systems:** Organisations need confidence that the external information systems contain the necessary security safeguards (i.e., security controls), so as not to compromise, damage, or otherwise harm organisational information systems.
- **Supply Chain Protection:** Information systems need to be protected throughout the system development life cycle. Protection of organisational information systems is accomplished through threat awareness, by the identification, management, and reduction of vulnerabilities at each phase of the life cycle and the use of complementary, mutually reinforcing strategies to respond to risk. Organisations consider implementing a standardised process to address supply chain risk with respect to information systems and system components, and to educate the acquisition workforce on threats, risk, and required security controls. Organisations use the acquisition/procurement processes to require supply chain entities to implement necessary security safeguards to reduce the frequency of unauthorised modifications at each stage in the supply chain and to protect information systems and information system components, prior to taking delivery of such systems/components.

# 5

# Compliance and Regulation

# 5.1.Protection of personal data in the finance sector

## 5.1.1. Objectives of personal data protection and why it is especially relevant in the finance sector

The fundamental rights to privacy and to the protection of personal data are enshrined in Articles 7 and 8 of the Charter of Fundamental Rights of the European Union[1] and are crucial to the protection of various other fundamental rights such as the right to communications, freedom of thought, freedom of expression, freedom to conduct business and the right to an effective remedy and to a fair trial.[2] However, the fundamental right to data protection is not absolute, but it rather has to be balanced against other fundamental rights according to the principle of proportionality.[3]

In the financial services sector, various kinds and great amounts of personal data are processed regularly in regard to bank customers and therefore, data protection is crucial.

As bank customers depend on access to financial services, availability and integrity of the finance s ector and the personal data held by financial service providers relating to them as individuals is important to ensure both the availability of these essential services important for daily life and the availability and functioning of the sector as a whole.

## 5.1.2. The scope of application of the General Data Protection Regulation in the context of customers of financial service providers

### What is personal data according to GDPR?

The General Data Protection Regulation (GDPR) applies to the processing of personal data wholly or partly by automated means or other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.[4] The definition of personal data encompasses any information relating to an identified or identifiable natural person, such as e-mail address, telephone number, name, date of birth, etc.

Data is being processed wholly or partly by automated means if it is not processed exclusively by manual processing activities, for example if data is automatically saved on a hard drive. The GDPR also applies if the data which takes places other than by automated means forms part of a filing system or is supposed to form part of a filing system, for example if data is collected manually and then systemized in a way which allows for structuring the set of data following at least two different criteria.[6] This is the case if banks and other financial institutions e.g. collect, store or transfer their customers' personal data on their server or systematically store it in their filing system.

1 Art 7 and 8 Charter of Fundamental Rights of the European Union.
2 Recital 4 Regulation (EU) 2016/679.
3 Recital 4 Regulation (EU) 2016/679.
4 Art 2 (1) Regulation (EU) 2016/679.
5 Maguire, R. (ed.) (2018) "Data protection: principles and main features," in Information Rights for Records Managers. Facet, pp. 73–98. doi: 10.29085/9781783302468.004., at 77.
6 Kühling/Raab, Art 2 18 in Kühling/Buchner, DS-GVO BDSG Kommentar [GDPR BDSG Commentary, 2nd edition 2018].

## 5.1.3. Obligations of the data controller according to GDPR

### Data protection principles

Principles relating to the processing of personal data are laid down in Article 5 GDPR; they are required to be fulfilled by the data controller whenever they are processing personal data.

**LAWFULNESS, FAIRNESS AND TRANSPARENCY**

Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject.

- Lawfully means that the data is processed in accordance with the GDPR and supporting national legislation. [7]
- Fairness means that the way the data is processed is communicated accordingly, not used contrary to the interest of the data subjects and not transmitted to third parties without the data subject being aware of this. [8]
- Transparency requires clearly communicating to the data subjects what data is processed to what ends and how [9]

**PURPOSE LIMITATION**

Personal data shall be "collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes [...]" [10]

7 R. Maguire (ed.) "Data protection: principles and main features," in Information Rights for Records Managers 73–98 (2018), at 78, doi: 10.29085/9781783302468.004.

8/9 R. Maguire (ed.) "Data protection: principles and main features," in Information Rights for Records Managers 73–98 (2018), at 78, doi: 10.29085/9781783302468.004.

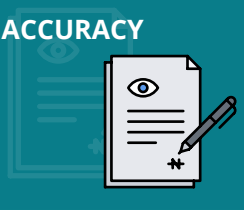
10 R. Maguire (ed.) "Data protection: principles and main features," in Information Rights for Records Managers 73–98 (2018), at 79, doi: 10.29085/9781783302468.004; Article 5 (1) lit b Regulation (EU) 2016/679.

**DATA MINIMIZATION**

Personal data collected are required to be "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed" [11]

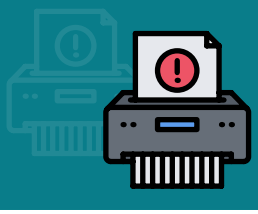
If the purpose of processing can be achieved with anonymized data, the data is required to be anonymized.[12]

**ACCURACY**



Personal data are required to be accurate and, where necessary, kept up to date; this principle is related to the rights of erasure and rectification as inaccurate personal data must be corrected according to Art 16 GDPR.[13]

**STORAGE LIMITATION**



When personal data is processed, it must not be kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the personal data are processed.[14] Personal data thus has to be destroyed if it is no longer necessary for a particular purpose.

**INTEGRITY AND CONFIDENTIALITY**

Personal data is required to be "processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction of damage, using appropriate technical or organizational measures".[15] The data has to be protected by means of information security and organizational measures, requiring a cooperation between information security staff and other staff in developing according policies, procedures and guidance.

11 R. Maguire (ed.) "Data protection: principles and main features," in Information Rights for Records Managers 73–98 (2018), at 80, doi: 10.29085/9781783302468.004.

12 Herbst, Art 5 55-57 in Kühling/Buchner, DS-GVO BDSG Kommentar [GDPR BDSG Commentary, 2nd edition 2018].

13 Herbst, Art 5 60-63 in Kühling/Buchner, DS-GVO BDSG Kommentar [GDPR BDSG Commentary, 2nd edition 2018]; Article 5 (1) lit d Regulation (EU) 2016/679; R. Maguire (ed.) "Data protection: principles and main features," in Information Rights for Records Managers 73–98 (2018), at 80, doi: 10.29085/9781783302468.004.

14 Herbst, Art 5 64-65 in Kühling/Buchner, DS-GVO BDSG Kommentar [GDPR BDSG Commentary, 2nd edition 2018]; R. Maguire (ed.) "Data protection: principles and main features," in Information Rights for Records Managers 73–98 (2018), at 81-82, doi: 10.29085/9781783302468.004; Article 5 (1) lit e Regulation (EU) 2016/679.

15 Art 5 (1) lit f Regulation (EU) 2016/679.

**INTEGRITY AND CONFIDENTIALITY CONTINUED**

What can I do?

"Inform your information security colleagues when a breach occurs [...]" [16] and "[...] follow the organization's mandated information security practices regarding encryption, managing passwords and security classifications [...]" [17]

**ACCOUNTABILITY**

Personal data are required to be accurate and, where necessary, kept up to date; this principle is related to the rights of erasure and rectification as inaccurate personal data must be corrected according to Art 16 GDPR.[18]

## Data subject rights

**RIGHT TO INFORMATION**

Article 13 – If personal data are collected from the data subject, the data subject has to be provided with – inter alia – the following information at the time when personal data are obtained:

- Identity and contact details of the controller
- Contact details of the data protection officer
- Purposes of processing for which the personal data are intended as well as the legal basis for the processing
- If processing of personal data is based on Art 6 (1) lit c, the legitimate interests pursued by the controller or by a third party
- Period for which the personal data will be stored
- The existence of the right to request from the controller access to and rectification/erasure of personal data or restriction of processing or objection to processing and the right to data portability.
- The right to lodge a complaint with the supervisory authority

16 R. Maguire (ed.) "Data protection: principles and main features," in Information Rights for Records Managers 73–98 (2018), at 83.
17 R. Maguire (ed.) "Data protection: principles and main features," in Information Rights for Records Managers 73–98 (2018), at 83.10
18 Art 5 (2) Regulation (EU) 2016/679.

**RIGHT OF ACCESS BY THE DATA SUBJECT**

Article 15 GDPR grants the data subject the right to access the personal data concerning him or her and also further information such as the purposes of the processing, the categories of personal data concerned, information about the right to request from the controller rectification or erasure of personal data or information about the right to lodge a complaint with a supervisory authority, inter alia.[19] The right to access entails the obligation of the controller to provide a copy of the personal data undergoing processing.[20]

**RIGHT TO RECTIFICATION**

According to Article 16 GDPR, the data subject has the right to have inaccurate personal data concerning him or her rectified without undue delay. [21]

**RIGHT TO ERASURE**

According to Article 17 GDPR, the data subject may request the erasure of personal data concerning him or her under certain circumstances, such as for example:

- If the personal data are no longer necessary in relation to the purposes for which they were processed
- If the data subject withdraws consent on which the processing is based according to Article 6 (1) lit a or Art 9 (2) lit a and where there is no other legal ground for the processing [22]

**RIGHT TO RESTRICTION OF PROCESSING**

Article 18 GDPR states that, under certain circumstances, data subjects shall have the right that the processing of their personal data be restricted, for example if the processing is unlawful and the data subject requests the restriction of processing of their data. [23]

19 Art 15 (1) Regulation (EU) 2016/679.
20 Art 15 (3) Regulation (EU) 2016/679.
21 Art 16 Regulation (EU) 2016/679.
22 Art 17 Regulation (EU) 2016/679.
23 Art 18 (1) lit b Regulation (EU) 2016/679.

**RIGHT TO DATA PORTABILITY**

Article 20 GDPR grants the right to data portability under certain conditions. The right to data portability shall be granted by providing the data subject with their personal data in a structured, commonly used and machine-readable format. The data subject may then transmit those data to another controller.[24] The right to data portability exists where the processing is based on (explicit) consent or on a contract and under the condition that the processing of the data is carried out by automated means. [25]

**RIGHT TO OBJECT TO PROCESSING**

According to Article 21 GDPR, the data subject has the right to object to processing of personal data concerning them which is based on the legal basis of either the performance of a task carried out in the public interest (Art 6 (1) lit e GDPR) or legitimate interests pursued by the controller or by a third party (Art 6 (1) lit f GDPR). From the objection onwards, the data controller shall not process the data unless he demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject. [26]

24 Art 20 (1) Regulation (EU) 2016/679.
25 Art 20 (1) Regulation (EU) 2016/679.
26 Art 21 Regulation (EU) 2016/679.

1

**JOINT CONTROLLERS' AGREEMENT**

Where the purposes and means of the processing of personal data are determined jointly by two or more controllers, an agreement shall lay down their respective responsibilities for compliance with obligations under the GDPR. Especially the respective responsibilities regarding the exercising of data subject rights and the complementary provision of information have to be transparently regulated.[27]

2

**DATA PROCESSING AGREEMENT**

Where the data controller charges another person or legal entity with processing personal data on their behalf, the processing of the personal data by this other person or legal entity has to be governed by a contract or similar. This is to ensure that data processing principles and data subject rights are accounted for appropriately. [28]

3

**RECORDS OF PROCESSING ACTIVITIES**

A record in writing, which may also be in electronic form, to be maintained by the controller which has to contain for example the following information:

- Name and contact details of the controller
- Purposes of processing
- Description of the categories of data subjects and of the categories of personal data
- Transfers/disclosures of personal data [29]

27 Art 26 Regulation (EU) 2016/679.
28 Art 28 (3) Regulation (EU) 2016/679.
29 Art 30 Regulation (EU) 2016/679.

## 4 MEASURES TO ENSURE THE SECURITY OF PROCESSING

Personal data has to be kept secure. How this security is to be achieved depends on the nature, scope, context and purposes of processing as well as the risks for and severity of the processing for the rights and freedoms of natural persons. Appropriate measures can be – inter alia:

- Pseudonymization and encryption of personal data
- Ensuring the ongoing confidentiality, integrity, availability and resilience of processing systems and services
- Regular evaluation of the effectiveness of technical and organizational measures to ensure the security of processing [30]

## 5 NOTIFICATION OF A PERSONAL DATA BREACH TO A SUPERVISORY AUTHORITY

If a personal data breach occurs, it has to be notified by the controller without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the breach to the competent supervisory authority. [31]

30 Art 30 Regulation (EU) 2016/679.
31 Art 33 Regulation (EU) 2016/679.