sciendo

Wroclaw Review
of Law, Administration & Economics
Vol 11:2, 2021
DOI: 10.2478/wrlae-2021-0013

Practical Methods of Implementation for the Indispensable Mechanism of GDPR Compliance

Michał Bańka, Tomasz Soczyński**, Dariusz Wasiak****

Keywords

GDPR, personal data breach, EU Data Protection Regulation, notification requirement, mandatory data breach notification, security breach notification, proceeding pseudonymization, anonymization encryption of personal data, proceeding system recovery and testing, business continuity plan

Abstract

New quality that has been delivered by the provisions of General Data Protection Regulation (GDPR) (EU) 2016/679 is intended to secure a higher level of safety for personal data processing operations. The following elaboration was produced as an attempt to address the questions regarding practical methods of implementation for the indispensable mechanism of GDPR compliance. The guidelines contained in the article are supposed to be helpful in enhancing the safety level for processed personal data. Theoretical and legal studies over the status and functioning of the valid legislation with reference to the practical application of personal data processing procedures have been applied in the article. The main sources of knowledge included valid legal acts, opinions from Article 29 Working Party, technical norms as well as available general knowledge. The outcomes of the said studies indicated the complexity of the issue and established the necessity to continue further studies in practical implementation methods, such as the national and European mechanism of certification or sector codes of good practices.

* Ph.D, PW IOSP, michal.banka@pw.edu.pl, https://orcid.org/0000-0003-0853-9687.
** Ph.D candidate, UG WPiA, tomek_soczynski@yahoo.com, https://orcid.org/0000-0002-0795-5067.
*** Ph.D, WSB University in Wrocław, dariusz.wasiak@wsb.wroclaw.pl, https://orcid.org/0000-0001-6057-7475.

Introduction

General Data Protection Regulation[1] (hereafter: GDPR) introduces the requirements for personal data protection based on two fundamental principles. The first principle, **risk-based approach,** assumes that the higher a risk related to personal data processing, the wider the scope of duties for a data controller. Effective application of the said principle requires the data controller to evaluate the risk related to personal data processing, both with regard to the identification of threats related to the processing and the infringement on the rights and freedoms of persons to whom the data refer. Risk evaluation is intended to prescribe actions that reduce risk to a minimum by using proper organisational and technical measures.[2]

In turn, **the principle of accountability** assumes that the data controller ought to be able to prove that the applied personal data processing methods remain in line with GDPR. Effective application of the principle of accountability requires the data controller to implement the relevant procedures and maintain the proper documentation, even if the obligation to possess it does not result from GDPR provisions directly. Implementation of such procedures and documentation will make it easier to prove that the requirements set forth by GDPR with relation to data processing and protection are met.

Both principles specified above originate from ISO/IEC standards. Risk evaluation in order to select the protective measures remains the basis of the standards related to information safety management (including ISO 31000, ISO/IEC 27005, ISO/IEC 29134). Accountability remains an equivalent of protection category defined by the standards as compliance. Its enforcement is related to providing compliance with the information protection principles accepted within an organisation (including ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 29151). It constitutes one of the basic principles of privacy set forth by the ISO/IEC 29100 standard. Throughout the GDPR, organisations that control the processing of personal data (known as *controllers*) are encouraged to implement protective measures corresponding to the level of risk of their data processing activities.[3]-[4]

---

1 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), [2016] OJ 119/1.

2 Martin Yod-Samuel, Antonio Kung, 'Methods and Tools for GDPR Compliance Through Privacy and Data Protection Engineering' 2018 IEEE European Symposium on Security and Privacy Workshops.

3 Edward Humphreys, *Implementing the ISO/IEC 27001: 2013 ISMS Standard* (Artech House 2016).

4 Olha Drozd, 'Privacy pattern catalogue: A tool for integrating privacy principles of ISO/IEC 29100 into the software development process' IFIP International Summer School on Privacy and Identity Management (Springer, Cham 2015).

I. Different Types of Risk

1.1. Low risk

Although the GDPR is silent on how organisations should assess and quantify risk, certain trends emerge from the sections where the risk does appear that will guide organisations into implementing a risk-based approach. The concept of risk appears to mean different things to different people, especially in a subjective domain such as privacy, and is often used flexibly to apply to different components of risk.

1.2. Risk

For activities that are not labeled high risk, controllers still must adopt measures that are appropriate to the risk level of the activity. For example, controllers are required to 'ensure a level of data security appropriate to the risk' and implement risk-based measures for ensuring compliance with the GDPR's general obligations.

1.3. High risk

The GDPR imposes heightened requirements on controllers that are engaged in high-risk activities. Specifically, before engaging in such an activity, an organisation may be required to consult data protection authorities and conduct a detailed privacy impact assessment. In case of a data breach, it may be required to notify the potentially affected individuals.[5]

II. Securing the Compliance of Data Processing with GDPR

Pursuant to article 32 of GDPR, while selecting the protection measures one must assess whether the degree of data safety provision remains adequate (using adequate protection categories), and whether it also includes the risk related to data processing resulting from random or unlawful data destruction, loss, or modification. These measures must protect against unauthorised disclosure or unauthorised access to personal data transferred, stored, or processed in another manner.

5 Gabriel Maldoff, 'The risk-based approach in the GDPR: interpretation and implications',< https://iapp.org/media/pdf/resource_center/GDPR_Study_Maldoff.pdf. , 2> accessed 1 April 2021 r.

As an example of proper technical and organisational measures for data protection, article 32 of GDPR specifies the following:

- Pseudonymisation and encryption of personal data;
- Ability to provide confidentiality, integrity at all times;
- Availability and durability of processing systems and services;
- Ability to restore personal data availability and access to data in case of a physical or technical incident;
- Regular testing, measuring, and assessment of efficiency for technical and organisational measures that are supposed to provide processing safety.

This catalogue of measures is not complete, and protection categories specified ought to be selected to meet the needs that originate from the risk assessment process.

In case of the requirement to assess the impact from planned processing operations on data protection, set forth by article 35 of GDPR, it is performed by the data controller under special circumstances only, including:

- Automated processing, including profiling, remaining the basis for a decision bearing legal consequences
- Large-scale processing personal data of special categories, such as health data, political data, and more
- Regular large-scale monitoring of places with public access.

The main element of impact assessment (PIA) is the evaluation of the risk of infringement on the rights or liberties of the persons to whom the data refer. If the risk is high, the measures planned to diminish the risk must be determined, including protections and safety mechanisms to safeguard personal data protection. While performing the risk assessment (PIA) and determination of protections, data controllers, as well as processing entities, may apply the guidelines contained in technical standards such as ISO/IEC 29100 or 27000.

III. Reporting the Data Protection Breach

GDPR includes, among other duties, the duty of the data controller to take proper actions when a personal data breach has been detected, including notification of a supervisory authority. Such duty shall apply to the majority of entities and is intended to enable the persons to whom the data refer to take proper measures to minimise potential threats.[6]

6 Nick Abrahams, Jamie Griffin, 'Privacy law: The end of a long road: Mandatory data breach notification becomes law' (2017) 32 Law Society of NSW Journal 76, < https://www.

3.1. What does a personal data breach include?

The definition contained in article 4 point 12 of GDPR specifies that a personal data protection breach means the infringement on safety leading to accidental or unlawful damage, loss, modification, unauthorised disclosure, or unauthorised access to personal data transferred, stored, or processed in any other manner. It seems obvious that the said infringement constitutes a safety incident that has a detrimental effect on the privacy of an individual.

3.2. General procedures related to personal data breaches

It must be noted that depending on the circumstances the breach may refer to confidentiality, availability, and integrity of personal data at the same time. Infringement on availability occurs when there has been a permanent loss or damage to personal data. Examples of the loss of availability include the cases when the data have been accidentally removed by an unauthorised person, or in the case of encrypted data, the key to decrypt has been lost. In cases when the data controller is unable to restore access to data, say from a backup copy, this is regarded as a permanent loss of availability. The loss of availability may occur also in case of serious disturbances in the proper functioning of services, power failure, or DDOS network attack, which make the personal data unavailable, permanently or temporarily.

When the personal data breach may bring about a high risk to the rights and liberties of physical persons, in line with the article 34 clause 1 of GDPR the data controller irrevocably passes to the data subject the information on the personal data breach.

Regardless of whether the supervisory authority must be notified of the breach or not, the data controller must store the documentation related to all personal data infringements, pursuant to article 33 clause 5 of GDPR.

The data controller will document all incidents and personal data breaches, including the description of the circumstances, its impact and the corrective measures taken. The documentation must allow for the supervisory authority to verify whether the said provision has been observed. This is related to the responsibility resulting from article 5 clause 2 of GDRP, which specifies that the data controller remains responsible for observation of provisions set forth by clause 1 and must be able to prove them being observed (accountability).

It seems justifiable that in order to secure compliance to articles 33 and 34 of GDPR, the data controller and a processing entity ought to develop documented

nortonrosefulbright.com/en-au/knowledge/publications/46f7c421/the-end-of-a-long-road-mandatory-data-breach-notification-becomes-law> accessed 1 April 2021 r..

procedures to be followed when an incident has occurred, together with the procedure to identify any breach and notify concerned parties. This may appear to be helpful in order to prove compliance with GDPR and to train the staff in the procedures to be taken in case of a breach.[7]

3.3. Incident management

Basic elements of the procedure to manage incidents include:

- Preparation, detection and reporting,
- Reply to incidents and improvement of the situation with regard to safety.

The incident management plan ought to be clear and concise, describing the steps to be taken, resources used and their roles, as well as time frameworks for the tasks to be completed.

Another important basis for effective incident management includes proper configuration of systems to register the evidence for an incident to have occurred, such as syslog and NTP time synchronisation for the systems generating the registers. Information on the data transferred, network flow, and firewall registers are generally more reliable than registers within the production system, especially when an intruder is able to change or, potentially, destroy the local registers.

Applied measures must be so effective as to make it possible for the personal data breach to be detected immediately. Such measures include technical solutions based on analysis of telecommunications traffic and automated logs analyses, such as DLP, IPS, or machine learning.[8]

3.4. Data Leakage Prevention (DLP)

DLP is a computer security term that is used to identify, monitor, and protect data in use, data in motion, and data at rest.[9] DLP is used to identify sensitive contents by using deep content analysis to peer inside files with the use of network communications. DLP is mainly designed to protect information assets with

---

7 Robert H.Sloan, Richard Warner, 'How Much Should We Spend to Protect Privacy?: Data Breaches and the Need for Information We Do Not Have' (2017), < https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3032143 > accessed 1 March 2021 r.

8 Teodor-Florin Fortiş, Victor Ion Munteanu, 'Topics in cloud incident management' (2017), <https://www.sciencedirect.com/science/article/abs/pii/S0167739X16305179 > accessed 1 April 2021 r.

9 Ma Jun et al., 'The application of Chinese wall policy in data leakage prevention', Communication Systems and Network Technologies (CSNT), 2012 International Conference on IEEE, < https://www.researchgate.net/publication/254035156_The_Application_of_Chinese_Wall_Policy_in_Data_Leakage_Prevention > accessed 1 April 2021 r..

minimal interference in business processes. It also enforces protective controls to prevent unwanted incidents. DLP can also be used to reduce risk and to improve data management practices, and even to lower compliance costs. Systems are designed to detect and prevent unauthorised use and transmission of confidential information. Vendors refer to the protocols as Data Leak Prevention, Information Leak Detection and Prevention (ILDP), Information Leak Prevention (ILP), Content Monitoring and Filtering (CMF), Information Protection and Control (IPC) or Extrusion Prevention System by analogy to Intrusion Prevention System.[10]

3.5. Intrusion Detection System (IDS)

IDS is a software or hardware component that automates the intrusion detection process. It is designed to monitor the events occurring in a computer system and network and responds to events with signs of possible incidents of violations of security policies. Intrusion Prevention System (IPS), on the other hand, is the technology of detecting intrusion or threat activities and taking preventive actions to seize them. It combines the knowledge of IDS in an automated manner.[11]

3.6. Machine learning in order to detect the threats

The security of our computer systems, network and data is continually at risk. The massive growth of the internet, and the proliferation of tools, tricks, and techniques for intruding and attacking systems and networks, has instigated the use of machine-learning-incorporated NIDS over the traditional ones. Machine learning algorithms are used for misuse detection and anomaly detection. In misuse detection, training data are labeled as normal or abnormal/malicious data, and then the classifier is trained to distinguish between the two.[12] The solutions to detect anomalies—for instance, data leakage, using machine learning function—

---

10 Bijayalaxmi Purohit Pawan Prakash Singh, 'Data leakage analysis on cloud computing' (2013) 3.3 International Journal of Engineering Research and Applications, < https://www.researchgate.net/publication/254035156_The_Application_of_Chinese_Wall_Policy_in_Data_Leakage_Prevention > accessed 1 April 2021 r.

11 Nilotpal Chakraborty, Intrusion detection system and intrusion prevention system: A comparative study [w:] 'International Journal of Computing and Business Research' (2013), <www.researchmanuscripts.com/May2013/1.pdf> accessed 1 March 2021 r. Madhuri Gokhale, 'Intrusion detection system and intrusion prevention system: A comparative study' [w:] Journal of Information Security (2021), http://ijsart.com/Content/PDFDocuments/IJSARTV67I241950.pdf> accessed 1 March 2021 r.

12 Rupali Malviya, Brajesh K. Umrao, 'Machine Learning Security' (2014), < http://inpressco.com/machine-learning-security/> accessed 1 March 2021 r.

may help to detect the nontypical events automatically and to transfer them to domain systems that monitor the incidents that have occurred.

The techniques applied are required to be effective, efficient, scalable, robust and capable of handling a high volume of data with high dimensionality and heterogeneity. A number of anomaly detection systems are being developed based on many different machine learning techniques. Some apply single learning techniques, such as support vector machines, genetic algorithms, neural networks, and so on. Other systems are based on combining different learning techniques. These are known as hybrid or ensemble techniques. These techniques are developed as classifiers, which are used to recognise whether the incoming traffic is normal or an attack. The research work concerned with security using machine learning technique is a vast area and still needs to be researched. In order to design more sophisticated classifiers, ensemble and hybrid classifiers can be examined and combined. Since the idea of coalescing multiple classifiers is to collaborate with each other instead of using contention and comparison, it is worth combining the two types for intrusion detection. The performance of machine learning algorithms depends upon certain factors. Feature selection is one of the important ones. Since there are a number of approaches to feature selection, which approach performs best for detection of intrusion and with which classification techniques is also a consideration.[13]

3.7. The policy to react to incidents

While developing the policy to react to incidents, the following must be specified:

- Principles for constant threat monitoring by means of the hacking detection systems and other monitoring applications.
- Principles to appoint a person or a team reacting to information safety incidents;
- Procedures to maintain, identify, react, assess, analyse and monitor information safety incidents
- The way to train the staff and to equip them with knowledge on the incidents related to information safety and required reactions
- The manner to communicate on the incidents related to information safety with reference to people outside and inside the organisation

The staff ought to be trained concerning the requirements posed by GDPR, the policy to react to incidents in the organisation. One must make sure that the staff understands the procedures to be taken in case of any breach.

13 Ibid.

IV. Procedures Related to Pseudonymisation and Encryption

GDPR recommends pseudonymisation of personal data as one of the measures for data collectors can use to diminish the risk of data processing operations.

4.1. Pseudonymisation

The definition of *pseudonymisation* set forth by article 4 point 5 of GDPR, means personal data processing in such a manner to make it possible to ascribe them to one, precise person (that is, a person to whom the data refer) without the use of any additional information. The required conditions are to store such data separately and to cover them by technical and organisational measures to exclude data attribution to an identified person or a person who can be identified. Pseudonymisation is not an animisation method. It only limits the ability to relate a data set with the original identity of the person whom the said data refer. Pseudonymised data cannot be identified with anonymous information, and remain personal data.

Pseodonymisation remains a method applied in order to diminish the probability that the personal data subject to this method accompanied by identifiers will make it impossible to identify a physical person. It is important though that the pseudonymisation process remains a reversible one: that is, that the identifiers do enable identification of the subject of the data.

Pseudonymisation cannot be confused with encryption, a data protection technique which is also recommended by GDPR, as it is something totally different. The pseudonymisation technique may be based on registering a piece of information in various unrelated database instances. It is the data controller who possesses a unique identifier to identify a given person. It may also be based on data replacement by pseudonyms, that is, by generating a combination of signs with the application of a one-way hash function, as demonstrated below.[14]

[14] Eric Verheul, Bart Jacobs, 'Polymorphic encryption and pseudonymization in identity management and medical research' (2017), < https://www.semanticscholar.org/paper/Polymorphic-Encryption-and-Pseudonymisation-in-and-Verheul-Jacobs/ff4578890218ce607cf86b9228f3d74c70090815> accessed 1 March 2021 r.

	Imię	Nazwisko	PESEL	Liczba Punktów	Wynik badania
2	Tomasz	Soczyński	8383838	34	Opisowy wynik badań
3	Tomasz	Soczyński	8383839	55	Badania
4	Tomasz	Soczyński	8383840	564	Wyniki
5	Tomasz	Soczyński	8383841	536	Opisowy wynik badań
6	Tomasz	Soczyński	8383842	44	Badania
7	Tomasz	Soczyński	8383843	42	Wyniki
8	Tomasz	Soczyński	8383844	786	Opisowy wynik badań
9	Tomasz	Soczyński	8383845	43	Badania

Imię	Nazwisko	PESEL	Liczba Punktów	Wynik badania
=TEXT(HASH(A3;"MD5")		d0d69bb627	34	Opisowy wynik badań
fcd7d475a01464a45	7029ef8afaf20d2603a	7b701387f1	55	Badania
fcd7d475a01464a45	7029ef8afaf20d2603a	5eed3b653	564	Wyniki
fcd7d475a01464a45	7029ef8afaf20d2603a	ec3fb2c8460	536	Opisowy wynik badań
fcd7d475a01464a45	7029ef8afaf20d2603a	12ae93cab	44	Badania
fcd7d475a01464a45	7029ef8afaf20d2603a	2082144c8	42	Wyniki
fcd7d475a01464a45	7029ef8afaf20d2603a	10360acb0	786	Opisowy wynik badań
fcd7d475a01464a45	7029ef8afaf20d2603a	749c2737b0	43	Badania

Figure 1: Example for the application of pseudonymisation

The essence of pseudonymisation is not encryption; it makes it impossible to decipher the features contributing to identification of a person, which allows proceeding with a set of pseudonymised information.

4.2. Encryption

Encryption is referred to as the process of changing an open text into a cryptogram. Mathematical functions, as well as the relevant sets of keys, as in the picture below, are used for encrypting and decrypting.

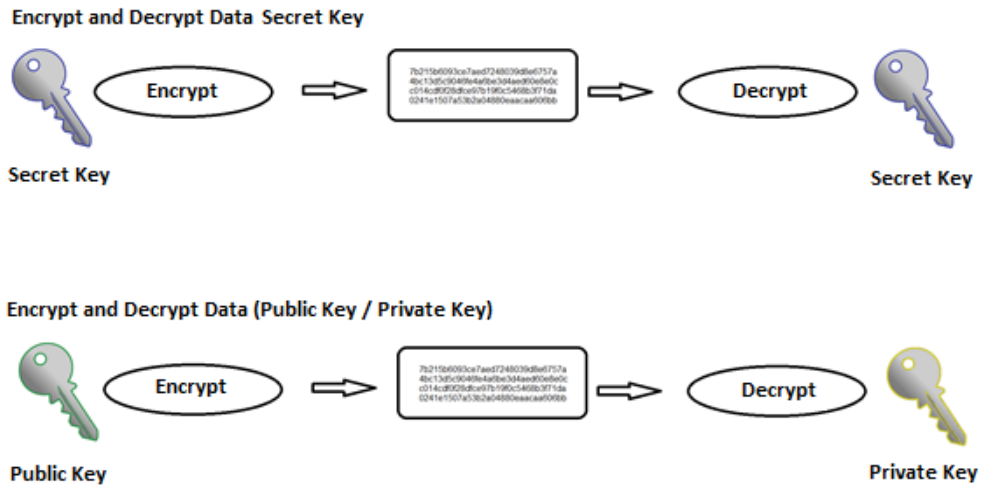

Figure 2: Visual demonstration of encryption

As one can see, encryption constitutes a strong tool in the protection of personal data against unauthorised disclosure. However, it limits, to a noticeable extent, the ability to analyse other data.

V. Continuity Plan/Security and Privacy

Identifying the continuity risks through organisation's Risk Management process will make managing and reducing the impact of these risks possible. It's important to ensure a plan to deal with the effects of risks that could appear. ICT systems and electronic data are essential components of the critical processes of an organisation and they should be particularly protected. Business Continuity process, described as the series of management operations, is used for maintaining the continuity of the fundamental processes of an organisation.[15]

Understanding which processes are critical and how quickly they must be restored is necessary to maintain the availability of IT and information. Organisation needs also to identify the required IT and information that keep these critical processes running. ICT and Information Security (IS) professionals, having received this information, should establish the actions that must be performed to prevent a disruptive event.

Due to the fact that risk is present in all decisions and activities undertaken by organisations, the approach to managing these continuity risks demands:

1. Proactive management of the risk, treating this as part of the organisation's Risk Management process on an ongoing basis. The aim is to develop the Business Continuity process which will highlight further risks and help minimise the likelihood or impact of an incident.
2. Implementation of a Business Continuity Management process in order to treat residual risk. Among the required outcomes of the Risk Management program, Business Continuity Management is one of the most essential. According to BS 25999-1 and the Draft for Public Comment BS 31100 – Code of Practice for Risk Management [BS 31100 DPC], Business Continuity helps to modify risk and minimise the impact if the risk occurs; especially in cases where avoiding, transferring or accepting the risk are not appropriate risk treatments.

Business Continuity Management is described in ISO 27001:2013 as a method of risk treatment, and as a measure to prevent interruptions to business activities and to protect critical business processes from the effect of major failures of information systems or disaster, as well as to ensure their timely resumption.[16]

---

15 <https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/bcm-resilience/it-continuity-home> accessed 1 March 2021 r.

16 <https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/bcm-resilience/bc-rm-interfaces > accessed 1 March 2021 r.

An important and helpful tool can be the national interoperability framework, which is the implementation of European regulations. There is a Polish example of the national interoperability framework.[17] §20 (2) to (14) ensures periodic internal audit of information security, at least once a year. The requirements regarding Business Continuity are deemed to be met if the information security management system has been developed on the basis of the Polish Standard PN-ISO/IEC 27001 and the establishment of safeguards, risk management and auditing is carried out on the basis of Polish Standards related to this standard, including:

1. PN-ISO/IEC 27002 with regard to the establishment of safeguards;
2. PN-ISO/IEC 27005 for risk management;
3. PN-ISO/IEC 24762 for the post-disaster iterability playback of the activity.

In order to bring practices into compliance with article 32 point 1 clause b of GDPR—the ability to provide constantly the confidentiality, integrity, availability and resistance of the processing systems and services—the data controller and a processing entity shall implement the relevant technical and organisational measures. This is done in order to provide the degree of safety corresponding to the type of risk, including the state of technical knowledge, implementation costs as well as character, range, context and objectives for the processing, and the risk of infringement on the rights and liberties of physical persons with a various probability of occurrence and importance of threat.

In order to minimise the risks defined, a continuity plan must be developed and implemented. While developing the plan, an analysis of which resources remain (including the infrastructure, internet connections or human resources of key importance for the functioning of the entire system) must be performed and potential threats must be identified.[18]

Such actions ought to allow for the development of the plan consisting of individual procedures relevant for the threats defined, for instance, the loss of personal data, data leak, or the failure of the internet connection.

17 <http://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20170002247/O/D20172247.pdf.> accessed 1 April 2021 r.

18 Alexander Setiawan, Adi Wibowo, Andrew Hartanto Susilo, Risk Analysis on the development of a Business Continuity Plan. Computer Applications and Information Processing Technology (CAIPT), 2017 4th International Conference on. IEEE, < https://www.researchgate.net/publication/323949453_Risk_analysis_on_the_development_of_a_business_continuity_plan > accessed 1 April 2021 r.

Table 1: Managing the continuity of operations – a permanent process (a template)

Activity	Description confirming the preparation
Performing the process risk analysis, including the inventory of assets	
Developing the scenarios for potential threats	
Developing the major continuity plan together with the appendices, compliant to ISO 22301	
Determination of the level of accepted risk together with the specification of potential losses, e.g., the threat of privacy loss by the data subjects	
Reconstruction of the processes to provide continuity	
Preparation of the plan for changes in the solutions possessed	
Preparation and testing of emergency plans/ procedures	
Appointing and training of staff	
Testing for the procedures accepted	
Evaluation of procedure appropriateness for the maintenance of operating continuity	

Pursuant to Article 32 point 1, clause c. of GDPR, the data controller and a processing entity shall implement the relevant technical measures, such as testing, measuring and assessment with regards to the effectiveness of the technical and organisational measure intended to provide personal data processing safety. For this purpose, the data controller ought to determine two extremely important factors: Recovery Point Objective (RPO) and Recovery Time Objective (RTO).[19]

RPO determines how long a break in service operations an entity can sustain and establishes the time for data timeliness. This factor enables evaluation of the risk of infringement on the right or liberties of physical persons.

RTO factor, in the case of a medical unit (e.g., a hospital), may equal minutes or seconds and the lack of immediate access to patient's personal data may determine their life or health. As for a housing community, RTO equaling hours or even days may be accepted and, probably, such a loss of availability may not bring about infringement on personal data. In this case, a backup copy made in daily intervals as RTO may prove to be correct. In order to evaluate RTO properly,

19 Ramani Ranjan Routray et al., 'Method and system for automated integrated server-network-storage disaster recovery planning' U.S. Patent No. 8, 121, 966. 21 Feb. 2012., < https://patents.justia.com/patent/20090307166> accessed 1 April 2021 r.

it is necessary to include RPO and the resources possessed, including the infrastructure remaining in our possession.[20]

Business continuity plans to process and launch an IT service continuity plan should include:

- Scope and purpose of the document
- Team definition of business units
- The role of the team of business units and their responsibilities.
- Assessment plans
- Incident contact information
- Criteria for the procedure
- Event assessment criteria
- Operating procedure, persons responsible for implementation
- Action Plan for a Response to Business Continuity
- Critical resource evaluation checklist
- Recovery plan for resources to be recovered
- Hardware retention policies
- Incident/ violation log
- Description of the flow of information
- Establishment of an incident management team

Business continuity plans and backup and recovery plans should put in place the procedures needed for functions to operate after a disastrous event and to bring all functions back to normal at the earliest possible time.

Disaster recovery plans should ensure that digital public services and their building blocks continue to work in a range of situations, such as cyberattacks or the failure of building blocks. Such planning should ensure interoperability and coordination over time when operating and delivering integrated public services by putting in place the necessary governance structure.[21]

The personal data controller, as well as a processing entity, are committed to develop a plan in case of a failure in providing individual services. If an incident jeopardises or excludes the maintenance of operational continuity with regard to personal data processing operations, it is necessary to apply the recovery procedures and restore the data and/or setups of devices from the last disrupted configuration. It is of extreme importance to review procedures of this kind on a regular basis.

---

20 Omar H.Alhazmi, Yashwant K. Malaiya, 'Assessing disaster recovery alternatives: On-site, colocation or cloud' Software Reliability Engineering Workshops (ISSREW), 2012 IEEE 23rd International Symposium on. IEEE, < https://www.researchgate.net/publication/233924171_Assessing_Disaster_Recovery_Alternatives_On-Site_Colocation_or_Cloud > accessed 1 April 2021 r.

21 <https://ec.europa.eu/isa2/sites/default/files/eif_brochure_final.pdf > accessed 1 May 2021 r.

The data controller is supposed to prepare the relevant technical and organisational measures to be applied in case of personal data processing system failure, especially:

- secure, in line with accepted procedure, steps to back up the services, systems, and applications as well as their configuration setups.
- store the backup copies in proper manner,
- if possible, store the backup copies in a different location
- guarantee the proper SLA level with regard to crucial points in the system infrastructure
- if so required, provide additional premises intended for crisis operations

The procedures should contain all information indispensable for the recovery of the services and specify persons responsible and their contact details.

The system administrator, in line with the accepted procedure, remains responsible for performing the regular tests with regards to the data integrity on backup copies.

The procedures to verify the correctness should consider:

- the correctness of the process to make a backup copy,
- correctness of the backup copy contents,
- coherence of the data for the occurrence of unauthorised values.

When errors have occurred during data integrity testing of backup copies, this fact should be registered and corrective measures ought to be taken up. It is necessary to make the test recovery of data copies within the environment separated from the production environment.[22]

Conclusions

Changes in the legislation regarding personal data protection resulting from the General Data Protection Regulation, remaining a part of the EU legislative amendment package, is supposed to provide a higher level of safety for personal data processing operations, including enhancing trust in digital services.

New mechanisms such as breach reporting and DPIA impose certain obligations on controllers and processors to ensure compliance with the principles set out in the provisions of the GDPR. The statistics presented by data protection authorities (e.g., data from the Personal Data Protection Office) seem to confirm

[22] William E. Sobel, Bruce McCorkendale, 'Restoration of backed up data by restoring incremental backup (s) in reverse chronological order' U.S. Patent No. 7, 802, 134. 21 Sep. 2010, < https://www.freepatentsonline.com/7802134.pdf > accessed 1 May 2021 r.

that private and public entities have difficulties in assessing what risk to the rights and freedoms of data subjects a given event may cause or whether it is a breach of data protection at all, as provided for in Article 33 of the GDPR[23]. In this context, it is important that data subjects are informed of any risks at the earliest possible stage, which will enable the necessary preventive measures to be taken to protect against the negative effects of a breach.

References

Abrahams Nick, Griffin Jamie 'Privacy law: The end of a long road: Mandatory data breach notification becomes law' (2017) 32 Law Society of NSW Journal.

Alhazmi Omar H., Malaiya Yashwant K., 'Assessing disaster recovery alternatives: On-site, colocation or cloud'. Software Reliability Engineering Workshops (ISSREW), 2012 IEEE 23rd International Symposium on. IEEE.

Chakraborty Nilotpal, 'Intrusion detection system and intrusion prevention system: A comparative study' (2013) International Journal of Computing and Business Research.

Drozd, Olha, 'Privacy pattern catalogue: A tool for integrating privacy principles of ISO/IEC 29100 into the software development process' IFIP International Summer School on Privacy and Identity Management (Springer, Cham 2015).

Fortiş, Teodor-Florin, Ion Munteanu Victor, 'Topics in cloud incident management' (2017).

Humphreys Edward, Implementing the ISO/IEC 27001: 2013 ISMS Standard (Artech House 2016).

Jun, Ma, et al., 'The application of Chinese wall policy in data leakage prevention'. Communication Systems and Network Technologies (CSNT), 2012 International Conference on. IEEE.

Maldoff Gabriel, 'The risk-based approach in the GDPR: interpretation and implications' IAPP https://iapp. org/media/pdf/resource_center/GDPR_Study_Maldoff. pdf.

Malviya Rupali, Umrao Brajesh K, 'Machine Learning Security' (2014).

Purohit, Bijayalaxmi, Pawan Prakash Singh, 'Data leakage analysis on cloud computing' (2013) 3.3. International Journal of Engineering Research and Applications.

Routray Ramani Ranjan et al., 'Method and system for automated integrated server-network-storage disaster recovery planning' U.S. Patent No. 8,121,966. 21 Feb. 2012.

Setiawan, Alexander, Wibowo Adi, Hartanto Susilo Andrew, 'Risk Analysis on the development of a Business Continuity Plan' Computer Applications and Information Processing Technology (CAIPT), 2017 4th International Conference on. IEEE.

Sloan, Robert H., Warner Richard 'How Much Should We Spend to Protect Privacy?: Data Breaches and the Need for Information We Do Not Have' (2017).

Sobel, William E., McCorkendale Bruce, 'Restoration of backed up data by restoring incremental backup (s) in reverse chronological order' U.S. Patent No. 7,802,134. 21 Sep. 2010.

[23] For example https://uodo.gov.pl/decyzje/ZSPR.440.43.2019 andhttps://www.uodo.gov.pl/decyzje/DKN.5131.3.2021/ accessed 1 May 2021 r.

Verheul Eric, Jacobs Bart, 'Polymorphic encryption and pseudonymisation in identity management and medical research' (2017).

Yod-Samuel Martin, Kung Antonio, 'Methods and Tools for GDPR Compliance Through Privacy and Data Protection Engineering' 2018 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW).