DATA BREACH IN EUROPE AND BEYOND

Authors. Tanja Breidecker. Francesca Caldani. Dariana-Sabrina Ilea. Endrit Shashaj. Carlo Mattina.

Tutor. Marta Marañón Hermoso

I. INTRODUCTION

Today, data breaches have become extremely common within the corporate world, especially considering the advances that are constantly being made in technology. Data breach constitutes one of the key risks of the cyber world, where sensitive data is constantly being transmitted over the internet. **This continuous transfer of information makes it possible for attackers in any location to attempt data breaches on almost any person or business they choose**. Data is also stored in digital form by businesses all over the world and the servers that store the data are often vulnerable to various forms of cyber-attack.

While cyber security incidents are becoming increasingly popular, as major corporations, companies and enterprises are prime targets for attackers attempting to cause data breaches, because they offer such a large payload, the security measures put in place by these organizations, although capable of mitigating the risks of security incidents, cannot completely avoid them.

In addition, the role of human error should not be overlooked by organizations and appropriate safeguarding measures should be taken to prevent human errors, due to their frequent appearance. Since these types of breaches can have both an intentional and unintentional source, it can be a challenge for data controllers to identify the vulnerabilities and adopt measures to prevent them.

Data breach constitutes a security incident in which data, like personal information and corporate data, are accessed, altered, erased, or disclosed without authorization. Such breaches have the potential to impact on the affected individuals' lives seriously and dramatically, including humiliation, discrimination, financial loss, physical or psychological damage or even threat to life.

Moreover, data breach consequences could be huge for companies. The financial impact of a data breach is undoubtedly one of the most immediate consequences that organizations will have to deal with. Data breach can affect or disrupt the operation of a company and result in loss of business. Other financial consequences include payment to affected customers for reimbursement and settlement as well as the costs for legal services, breach response and investigation, investment into new security measures, legal fees, not to mention the eye-watering regulatory penalties that can be imposed for non-compliance with the GDPR. Data breach can also cause serious damage to the brand and reputation of a company, projecting a negative image to the existing and potential customers. Clients and business partners may lose their trust and terminate their relationship with the companies.

In the current digital era, the protection of personal data has become a fundamental right recognized by various countries, which promulgated laws and regulation to guarantee the protection of physical persons. With the start of the new century the number of incidents involving data breaches and otherwise neglectful and unlawful behavior of data processors has increased dramatically. Consequently, EU regulators began questioning the adequacy of previous legal frameworks and proposed a new approach.

The New General Data Protection Regulation (GDPR) of the European Union came into force on May 25th, 2018, in replacement of the 1995 Data Protection Directive.[1] The new Regulation harmonized data protection rules across the EU and, additionally, promoted free flows of personal data within the Single Market while strengthening the rights of individuals concerning the usage of their personal data.

The GDPR has had a significant impact on data protection policy and enforcement beyond the EU and became a model for many national laws, including Chile, Japan, Brazil, South Korea, Argentina, and Kenya, with the ambition to protect persons and grant rights to transparency and control over the collection of personal information by companies and organizations.

The GDPR has introduced a new age of data protection requirements on business. On one hand, the requirement for organizations to put in place appropriate technical and organizational measures. By using these measures, personal data shall be processed in a manner to ensure the appropriate security, including protection against unauthorized or unlawful processing and against accidental loss, destruction, or damage. On the other hand, **the obligation to notify personal data breach to the competent national supervisory authority and, in certain cases, to communicate the breach to the individuals whose personal data have been affected by the breach**.

II. EXECUTIVE SUMMARY

In the following paper we highlight the relevance for companies to be diligent and comply with the double obligation resulting from the General Data Protection Regulation in order to limit the risks of potential data breaches. On one hand, **companies must adopt technical and security measures that minimize any risk**. On the other hand, **companies are obliged, in the event of an attack, to be transparent with the authorities and data subjects and, where appropriate, to report data breaches**. In turn, they must be able to take corrective measures that demonstrate proactivity and diligence towards the authorities.

The risk of a cyber-attack is inevitable for any company, but if we are able to demonstrate diligence and proactivity, the risk is greatly minimized and fines such as those already imposed on companies like British Airways or Marriott will be avoided. All of this is without prejudice to the reputational impact that this type of sanctioning proceedings undoubtedly entail.

The final question we pose in this paper is the following: are the obligations resulting from articles 33 and 34 of the GDPR regarding data breaches obligations of result or obligations of means? Our conclusion is that they are obligations of means. Indeed, we believe that it is not necessary to prove that a cyber-breach has been prevented (as, in practice, this is sometimes unavoidable). What is important is to show that the company has been diligent enough to take measures to minimize any risk to this effect and, of course, that the company has acted transparently with the authorities and stakeholders.

[1] Unlike a directive, a regulation does not have to be implemented in the national laws of the EU Member States: the GDPR leads to a completely harmonized regime in the EU.

III. DATA BREACH ACCORDING TO THE EUROPEAN GENERAL DATA PROTECTION REGULATION

1. The New General Data Protection Regulation (GDPR)

The New General Data Protection Regulation (GDPR) came into force on May 25th, 2018, with the aim to harmonize data privacy laws across all the European countries as well as providing greater protection and rights to individuals. The new Regulation introduced provisions and requirements related to the processing of personal data of individuals (formally called data subjects) who are located in the European Union, but it applies to any enterprise -regardless of its location and the data subjects' citizenship or residence - that processes the personal information of individuals inside the European Union.

The GDPR applies when personal data of natural persons are "processed".[2] The concept of personal data is much broader than personally identifiable information.[3] Any data that directly or indirectly identifies a person or could identity a person in the future, whatever their nationality or place of residence, is a personal data.[4] Consequently, whenever a party processes data that relate to a natural person that directly or indirectly identifies that person - whether the data is public or private, sensitive or non-sensitive[5] and whether identification is possible now or in the future - it processes "personal data" within the meaning of the GDPR.

The GDPR distinguishes between several parties responsible for upholding the rules and obligations under the EU data protection framework, with different duties and liabilities. The most important parties are the data controller and the data processor. The data controller is the natural or legal person who, alone or jointly with others, declare the lawful basis[6], determine the purposes and hand the means of the processing of personal data. The data processor, instead, is a legal or a natural person, agency, public

---

[2] Almost everything that can be done with personal data, such as storing, analyzing, selling, and even deleting personal data, falls within the definition of "processing". Under GDPR regulation, just some types of processing are excluded by the scope of the Directive: for example, there are exemption for "purely personal or household activity" and for processing activities concerning national security. There is also a special regime for freedom of expression and for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes.

[3] Examples of personal identifiable information are name, identification number, address, location data, online identifier (email or IP address), health, physical, genetic or biometric data, mental, economic, cultural or social identity of a natural person.

[4] See Article 29 Working Party, 'Opinion 4/2007 on the concept of personal data' (WP 136), 20 June 2007; Schwartz PM and Solove DJ, *The PII Problem: Privacy and a New Concept of Personally Identifiable Information* (2011) 86 New York University Law Review 1814.

[5] The processing of special categories of personal data is prohibited by default according to GDPR's Article 9. Racial, ethnic origin, political opinions, religious or philosophical beliefs, genetic data, biometric data, health, a natural person's sex life or sexual orientation can be counted as sensitive data. The GDPR lists some circumstances which allow organizations to process a special category of personal data.

[6] No personal data may be processed unless this processing is done under one of the six lawful bases specified by the regulation (consent, contract, public task, vital interest, legitimate interest or legal requirement). When the processing is based on consent the data subject has the right to revoke it at any time.

authority, or any other body who processes personal data on behalf of a data controller. A company can act both as a controller and as processor, depending on the exact type and usage of data. Furthermore, GDPR imposes an obligation on public authorities, companies processing sensitive personal data or data at a large scale[7] to employ or train a data protection officer (DPO). The DPO must take measures to ensure GDPR compliance throughout the organization.

When the GDPR applies to a data processing, the data controller is the primarily responsible for upholding the data protection principles and must ensure that the process accords with the GDPR's minimum standards of legitimacy.

When data is collected, data subjects (the person that can be identified through the personal data) must be clearly informed of their privacy rights under the GDPR and about the extent of data collection, the legal basis for processing of personal data, how long data is retained, if data is being transferred to a third-party and/or outside the EU, and any automated decision-making that is made on a solely algorithmic basis. The GDPR, indeed, aims to empower data subjects by granting them various rights, such as the right to access, rectify, and erase personal data, and the right to object to, or restrict, processing[8]. As such, the data subject must also be provided with contact details for the data controller and their designated data protection officer, where applicable.

The GDPR aims to protect personal data of individuals in the EU, however, the impact of the GDPR goes far beyond the EU and even organizations located outside the European Union could be subject to the requirements of the regulation. The law, indeed, applies to organizations that handle personal data of persons located in the European Union whether they are EU-based organizations or not (this is known as "extra-territorial effect"). The territorial scope of GDPR is determined by Article 3 and represents a significant evolution of the EU data protection law. Article 3 of the GDPR reflects the legislator's intention to ensure comprehensive protection of the rights of data subjects in the EU and to establish, in terms of data protection requirement, a level playing field for companies active on the EU markets, in a context of worldwide data flows.

The general rule is that GDPR applies to the processing of personal data in the context of the activities of an establishment based in Europe, regardless of whether the processing takes place in the EU or not (establishment criterion). But GDPR applies also to organizations that are not based in the EU and that process personal data of persons located in the EU (targeting criterion). This extension of the law's effects take place where the processing activities relates to the offering of goods or services to such persons in the EU[9] or to the monitoring of their behavior, as far as their behavior takes place within the Union. Where the GDPR applies to a non-EU controller or processor, there is an obligation on the controller or processor to appoint a representative in the EU, to serve as a point of contact for their obligations under the regulation and ensure compliance with GDPR.

---

[7] See Article (37)

[8] In short, when processing personal data, in order to be compliant under the GDPR data controllers have to respect seven rights of the data subject: the right to access; to data portability; to rectify data; to stop processing; to object; to erase data; and to resist profiling.

[9] The GDPR applies to data controllers or data processors not established in the EU when a natural or legal person offers goods or services to such data subjects in the Union, irrespective of whether a payment of the data subject is required.

The GDPR also regulates the data flows to countries outside the EU[10]: the GDPR forbids the transfer of the personal data of EU data subjects to countries outside of the European Union. The data transfer to third country is only allowed if there are imposed appropriate safeguards[11] that ensure compliance with data protection requirements and the rights of the data subjects[12], or if the third country's data protection regulations are formally considered adequate by the European Commission.

2. Obligation to put in place adequate security measures and the accountability principle

One of the requirements of the GDPR is that security of personal data shall be ensured throughout the processing of personal data, including protection of personal data against unauthorized or unlawful processing and accidental loss, destruction, or damage.[13]

In accordance with the integrity and confidentiality principle, the GDPR requires both controllers and processors to have in place appropriate technical and organizational measures to ensure a level of security appropriate to the risk posed to the personal data being processed. The security measures can include pseudonymization and encryption of personal data, ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services, the ability to restore the availability and access to personal data in a timely manner in case of an incident, as well as periodical testing of the security measures implemented.[14]

In implementing these technical and organizational measures, the controller and the processor should consider the state of the art, the costs of implementation and the nature, the scope, context and purposes of processing, as well as the risk of varying

[10] Article 44 GDPR.

[11] Binding corporate rules, standard contractual clauses for data protection, or a scheme of binding and enforceable commitments by the data controller or processor situated in a third country, are examples.

[12] Including the availability of enforceable data subject rights and of effective legal remedies, including to obtain effective administrative or judicial redress and to claim compensation, in the Union or in a third country

[13] Article 32 Security of processing 1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate: (a) the pseudonymisation and encryption of personal data; (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; (c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; (d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing. 2. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed. 3. Adherence to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate compliance with the requirements set out in paragraph 1 of this Article. 4. The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by Union or Member State law.

[14] See Articles 5(1)(f) and 32.

likelihood and severity for the rights and freedoms of natural persons. Moreover, the GDPR requires all the appropriate technological protection and organizational measures to be in place to establish immediately whether a breach has taken place, and consequently, to assess if the supervisory authority and the affected individuals should be notified of the breach.

Article 32 does not establish a closed list of security measures to be taken by companies to avoid data breaches. However, companies are required to be proactive and to adopt the necessary security measures to cover the risks resulting from the different types of processing. Moreover, the GDPR requires that every organization can demonstrate that their processing activities are in line with the data processing principles determined by the GDPR. In particular, the accountability principle in Article 5 (2) means that controllers are responsible for and should be able to demonstrate their compliance with the GDPR data processing principles listed in Article 5 (lawfulness, fairness, and transparency; purpose limitation; data minimization; accuracy; storage limitation; integrity and confidentiality and accountability).[15]

There are several things organizations should do to demonstrate accountability under the GDPR, such as create data protection policies, draw up contracts between data processors and data controllers, implement appropriate security measures, appoint a data protection officer, record all data processing activities, report data breaches, respond to data subject access requests, and complete data protection impact assessments.

[15] Art. 5:
1. Personal data shall be:
(a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency'); (b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation'); (c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation'); (d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy'); (e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation'); (f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').
2. The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').

3. Personal Data Breach under the GDPR

A personal data breach is defined by the GDPR in Article 4 (12) as *"a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed."*

While a breach is a type of security incident, the GDPR only applies where there is a breach of personal data that results in the inability of the data controller to ensure the observance of the key principles of personal data processing, for which the controller is responsible as laid out by Article 5 of the GDPR. It should be noted that while all personal data breaches are security incidents, not all security incidents are necessarily personal data breaches. Moreover, a security incident is not limited to the action of external threats where an attack is made on an organization from an outside source but may also include incidents from internal processing that breach security principles.

Regarding the effects of such a breach on the targeted personal data, "destruction" of personal data means that the data no longer exists, or no longer exists in a form that is of any use to the controller. "Damage" of personal data occurs when the data has been altered, corrupted, or is no longer complete. The "loss" of personal data should be interpreted in the sense that while the data may still exist, the controller has lost control or access to it, or no longer has it in its possession. Finally, "unauthorized or unlawful processing" is any form of processing which infringes with the GDPR and may include unauthorized access to personal data or disclosure of personal data to recipients who are not authorized to receive the data.

Article 29 Working Party ("WP29"), in its Opinion 03/2014 on breach notification, categorized breaches according to the following three main categories, based on information security principles:

- "Confidentiality breach" - where there is an unauthorized or accidental disclosure of, or access to, personal data.
- "Integrity breach" - where there is an unauthorized or accidental alteration of personal data.
- "Availability breach" - where there is an accidental or unauthorized loss of access to, or destruction of, personal data.

The three categories are not mutually exclusive and, based on the circumstances, a breach can also be a combination of two or all the above.

Therefore, controllers and processors should have a proactive approach and put in place processes to be able to react promptly in case of a breach, starting with the detection and containment of the breach, assessment of the risk to individuals, and then determining whether it is necessary to notify the competent supervisory authority, and to communicate the breach to the individuals concerned when necessary. Notification of the breach should also be included in the incident response plan. It is also recommended, in order to show compliance with the GDPR, that the controllers and processors have taken measures to be able to demonstrate that their employees have been trained on these procedures on how to react in case of a breach.

These procedures are a useful tool to plan effectively in case of a breach and determine the responsibilities within the organization for managing a breach and how to escalate an incident. As WP29 states in its Guidelines on Personal data breach notification under

GDPR, the focus of any breach response plan should be on protecting individuals and their personal data. A key point of any data security policy is being able to prevent the occurrence of breaches of all types and, if a breach does take place, to react promptly.

Based on the accountability principle, the controller must keep documentation of all breaches, regardless of whether they are required to notify or not.[16] Therefore, controllers should establish an internal register of all breaches, independently from whether a breach needs to be notified to the supervisory authority, taking into account that the controller can also be requested by the supervisory authority to show these records. WP29 also recommends that the controller should include in the register its reasoning for the decisions taken in response to a breach, regardless of the decision taken, and proper justification and evidence should be shown to support that decision.

4. Article 33 - Notification to the supervisory authority

In case of a personal data breach, the GDPR provides the obligation of the controllers of personal data to notify the breach to the competent national supervisory authority or to the lead authority, in case of a cross-border breach. In certain cases, the controller is also required to communicate the breach to the individuals whose personal data have been affected by the breach. The requirement to notify the supervisory authority and/or the individuals affected by the breach is not mandatory when the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.

In order to evaluate whether a personal data breach has to be notified to the supervisory authority and the individuals affected, the controller must be able to identify a breach and assess the risk to individuals, as is also emphasized in Recital 87 of the GDPR:

"It should be ascertained whether all appropriate technological protection and organizational measures have been implemented to establish immediately whether a personal data breach has taken place and to inform promptly the supervisory authority and the data subject. The fact that the notification was made without undue delay should be established taking into account in particular the nature and gravity of the personal data breach and its consequences and adverse effects for the data subject. Such notification may result in an intervention of the supervisory authority in accordance with its tasks and powers laid down in this Regulation."

A breach regarding personal data can conceivably affect individuals in a wide array of manners, and can result in physical, material, or non-material damage to the affected individuals, such as loss of control over their personal data, limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorized reversal of pseudonymization, damage to reputation, and loss of confidentiality of personal data protected by professional secrecy.

Accordingly, the GDPR requires the controller to notify a breach to the competent supervisory authority, unless it is unlikely to result in a risk to the rights and freedoms

[16] Article 33(5) states:
"The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with this Article."

of individuals[17]. Where there is a likely high risk of these adverse effects occurring, the GDPR requires the controller to communicate the breach to the affected individuals as soon as is reasonably feasible[18]. Processors also have an important role to play, as they must notify any breach to their controller as soon as it becomes aware of the breach so that the controller can fulfill its` obligations regarding the breach and notify the supervisory authority if necessary. The requirements for reporting the breach to the controller should be detailed in the contract between the controller and processor as required under Article 28 of the GDPR.

On the other hand, when a breach is unlikely to result in a risk to the rights and freedoms of natural persons, the notification of the supervisory authority and of the individuals is not required.

That would be the case, for example, when the affected personal data is protected by state-of-the-art security measures such as encryption and the data remain unintelligible while the availability of the data is not affected because there is a backup of the data, then it is unlikely that the breach constitutes a risk for the rights and freedoms of the individuals. However, if there are no backups of the encrypted personal data then there will have been an availability breach that could pose risks to individuals and may require notification. Similarly, a risk to individuals might occur even if backups of the data exist, but the restoration of data is not possible in a timely manner depending on the length of time in which restoration is complete and the effect that the lack of availability until restoration has on the individuals` rights and freedoms.

It should be underlined that data breach documentation in accordance with Article 33 (5) is a legal obligation, irrespective of whether the breach should be notified to the supervisory authority and/or the affected individuals or not.

The GDPR contains provisions on when a breach needs to be notified, and to whom, as well as what information should be provided as part of the notification.

Firstly, the controller has the obligation to act on any alert of a potential breach, to contain the incident and to conduct investigations in order to establish whether there is in fact a breach and collect relevant information. If the controller finds with a reasonable degree of certainty that a breach has indeed occurred, thus becoming ‘aware’ of the data breach, is must then notify the supervisory authority without undue delay, but not later than 72 hours if feasible. If the controller fails to notify the supervisory authority, it must give justification as to the reasons of the delay: the fact that the notification was made without undue delay should be established taking into account in particular the nature and gravity of the breach and its consequences and adverse effects for the data subject. However, when further investigation is needed, and it is not possible to investigate a breach fully before reporting in order to understand exactly what has happened and what needs to be done to mitigate the breach, Article 33(4) of the GDPR provides that the information to the supervisory authority may be provided in phases. This means that, after making an initial notification, a controller could update the

17 *i.e.* the rights enshrined in the Charter of Fundamental Rights of the EU

18 Article 33(1) provides that:

“In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.”

supervisory authority to add information to the ones already given. This rule aims to ensure that controllers act promptly and seek relevant advice from the supervisory authority.

In managing a personal data breach, it is required that the potential risk of the incident is determined, as well as the extent of the potential impact on the individuals to be estimated. The risk will depend on a wide array of factors and the specific combination of these factors, ranging from the type of breach, the nature, sensitivity, and amount of data affected, ease of identification of affected individuals, the severity of the consequences for the individual, the number of affected individuals, as well as the special characteristics of the affected individuals and the data controller.

Notifications to the supervisory authority should be clear, concise, and include the information necessary for it to be adequately analyzed. The notification should contain, firstly, a description of the nature of the personal data breach including, where possible, the categories and approximate number of data subjects concerned, and the categories and approximate number of personal data records concerned.

Moreover, one of the key elements the controller should include in the notification is a description of the likely consequences of the personal data breach. The controllers should consider and describe not just likely consequences, but also possible consequences, as the risk of consequences occurring may become more likely over time.[19]

Controllers will also describe the measures taken or proposed to be taken to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects on individuals. It is very important to explain to the authority whether there have been any deficiencies from the point of view of security measures and whether the controller has taken measures to remedy or mitigate the identified deficiencies[20]. The more proactive and the more solutions are proposed at an early stage, the lower the risk of a sanction for the company.

Furthermore, the identity of the Data Controller and the Data Protection Officer (or a contact person if a Data Protection Officer has not been assigned) must be transmitted to the supervisory authority.

It should be underlined that a failure to report a breach where such a notification is mandatory according to Article 33 and/or 34, either to the individuals affected by the

[19] For instance, if personal data was secured with state-of-the-art encryption at the time of the breach, so there would likely be no consequences, however if later a serious vulnerability in the encryption used is later discovered, then the consequences are more likely.

[20] Containment measures may include: stopping the system if the data breach is caused by system failure; changing the users' passwords and system; configurations to control access and use; consider whether technical advices or assistance be immediately sought internally or from outside to remedy the system loopholes and/or stop the hacking; ceasing or changing the access rights of individuals suspected to have committed or contributed to the data breach; notifying the relevant law enforcement agencies if identity theft or other criminal activities were or likely to be committed.

breach or to the supervisory authority or both, may entail a sanction to the controller under Article 83 of the GDPR[21].

As such, the supervisory authority may impose an administrative fine up to 10,000,000 EUR or up to 2 % of the total worldwide annual turnover of the undertaking, as well as an additional corrective measure, if necessary.

In some cases, the failure to notify a breach is brought upon by either an absence of security measures or an inadequacy of the existing security measures, which during the investigation can be revealed to the supervisory authority. If so, the supervisory authority can also issue a fine for the absence of or inadequacy of security measures provided in Article 32, as a separate infringement.

The notification requirement introduced by the GDPR is a fundamental tool to guarantee that the processing procedures are in line with the data protection principles set out by the law and encourage controllers to act promptly on a breach, contain it and, if possible, recover the compromised personal data, and to seek relevant advice from the supervisory authority. The notification requirement can also help companies to put in place a comprehensive, flexible data breach response solution that can help protect reputation, mitigate potential damages, and rebuild trust and confidence with potentially impacted consumers.

5. Article 34 – Communication to the data subjects

Article 34 of the GDPR provides that when it is likely that a personal data breach poses a high risk for individuals' rights and freedoms, the data controller has the obligation to communicate with the affected individuals (the data subjects) without undue delay.

The notification to the data should be made in close cooperation and under the guidance of the supervisory authority. When notifying the supervisory authority, controllers can receive advice from the authority on whether the affected individuals need to be informed and if so, if the communication with the individuals can be postponed in case such communication could interfere with the results of the ongoing investigation regarding the breach. Moreover, the supervisory authority may order the controller to inform the affected individuals about the breach if the controller has not done so already.

When the controller communicates a breach to the affected individuals, it should be transparent about the breach and communicate in an effective and timely manner, using simple and concise language. Communication of the breach to individuals also allows individuals to be informed on the nature of the data breach, a description of the risks presented as a result of the breach steps taken to address the breach and the steps the individuals can take to protect themselves from its potential consequences according to the information that the controller provides. Accordingly, it would help the controller to demonstrate accountability and compliance by retaining evidence of such communication.

---

[21] According to WP29 guidelines on administrative fines: “The occurrence of several different infringements committed together in any particular single case means that the supervisory authority is able to apply the administrative fines at a level which is effective, proportionate and dissuasive within the limit of the gravest infringement”.

The notification should be addressed directly to the data subject and only if direct communication implies technical or organizational effort that is disproportionate in relation to the consequences of the data breach, in which case a public notice or press release would be an alternative. Such would be the case of a company which suffers a data breach that affects a large number of customers as, for example, happened in the Marriott International case in 2018 (detailed below), when Marriott International announced that attackers had stolen data on approximately 500 million customers. The compromised data consisted in a combination of contact information, passport numbers, guest numbers, travel information, and other personal information, as well as, in the case of more than 100 million customers, credit card numbers and expiration dates. In cases as the one described, communicating the data breach individually to each customer could be very complicated and could cause major problems for the customers who receive such a communication. The publication of a general communication in a medium accessible to the interested parties can be a solution to ease the logistical problems and help mitigate the individual impact of such communications.

However, it would not be necessary to communicate with data subjects if the data controller has put in place adequate technical and organizational measures to ensure data protection before the breach has taken place or if after the data breach the data controller has taken protective measures that mitigate the potential impact on data subjects and ensure that the high risk would not be imposed.

In conclusion, regardless of the nature of the business, storing and safeguarding clients as well as employee data is imperative.

For any business, perhaps the one of the biggest long-term consequence of a data breach is the loss of customers` and employees` trust, as a good reputation is often a company's most prized asset. However, even one compromising episode of a data breach may tarnish even the best of reputations. This could have a profound and lasting effect on a company, since consumers must be able to trust the business` security practices to become a customer, which in most cases nowadays requires them to entrust them with their personal information.

But data breaches not only impact a business's reputation, potentially damaging its relationship with customers and employees, it may also trigger significant legal liability and make the business a target of data breach claims or lawsuits, on top of the risk of investigation of the supervisory authority and administrative fines. Taking responsibility for how they handle personal data, and the ability to demonstrate the steps taken to protect individual`s rights results in better legal compliance, but also offers businesses a competitive advantage. As such, accountability is regarded as a real opportunity to develop and sustain people's trust. Furthermore, being able to show that the business has assessed the risks and adopted adequate measures and safeguards can help with mitigation against potential investigation, claim or lawsuit, since the supervisory authority is required to consider the technical and organizational measures the data controller had in place when considering an administrative fine.

As personal data breaches may cause real harm and distress to individuals and individuals are entitled to be protected from these consequences, they can claim compensation if a company or organization did not respect the data protection measures and, as a result, they suffered material damages (such as financial loss) or non-material damages (such as distress, or loss of reputation). Data breaches are becoming an increasing focus for litigation, and collective actions are growing in number, as all companies use personal data, and therefore risk being faced with these claims.

In this regard, collective data actions are of particular concern for companies. Although the individual claims awarded by the courts appear relatively small, ranging from hundreds to a few thousand euros, if a large customer base has been affected, and those customers join forces to claim as a group, they can have a significant financial impact on an organization and could even surpass in figures any regulatory penalty.

In addition, as the case of Lloyd v Google LLC [2019][22] demonstrates, claimants may not need to have suffered financial loss or distress to claim for misuse of their data. In this case, which is a collective action against Google in the United Kingdom for allegedly tracking the BGI of 4.4 million iPhone users to sell to advertisers, the Court of Appeal found that claimants are entitled to bring a claim simply for loss of control over their personal data, which is in itself damage, for which compensation must be paid, even where they are not claiming or cannot demonstrate financial loss or distress that has resulted from the breach. Moreover, companies may face claims even where the supervisory authority has not taken enforcement action.

Although initially it seemed to some that there was not much reason for concern about the trend of class actions in this area, in the light of such recent rulings, they now seem to become an ever more present reality which companies must take into consideration when dealing with protection of personal data.

[22] See the ruling of the British Court of Appeal of 2 October 2019 via https://www.judiciary.uk/wp-content/uploads/2019/10/Google.finaldraftjudgment. approved-2-10-19.pdf.

IV. SANCTIONS IN EUROPE FOR DATA BREACHES

Since the GDPR came into effect in May 2018, great emphasis was placed on the related violations.

According to various international research, between January, 2020, and January, 2021:

- *GDPR fines rose by nearly 40%;*
- ***Data protection authorities recorded 121,165 data breach notifications (19% more than the previous 12-month period);***
- *Penalties under the GDPR totaled €158.5 million*.

This represents a 39% increase compared to the 20 months the GDPR was previously in force since May 25th, 2018. Since that date and up to January 2021, a total of € 272.5 million in fines have been imposed across Europe under GDPR, with a prominent role played by the (i) Italian authority (€ 69.3 million), (ii) German authority (€ 69.1 million), and (iii) French authority (€54.4 million).

This calculation does not include two fines against Google LLC and Google Ireland Limited totaling € 100 million (€ 60 million + € 40 million) and a fine of € 35 million against Amazon Europe Core issued by the French data protection authority "CNIL" ("Commission nationale de l'informatique et des libertés") on December 10th, 2020, as proceedings on these fines are still pending before the Conseil d'Etat.

The above being said, the largest fines imposed so far related to data breach are the following:

Company	GDPR fine
❖ **H&M**	**€35,258,708**
❖ **British Airways**	**€22,046,000**
❖ **Marriott International**	**€20,450,000**
❖ **Air Europe**	**€600,000**

H&M GDPR fine - €35,258,708

On October 5, 2020, the Data Protection Authority of Hamburg, Germany, fined clothing retailer H&M €35,258,707.95 — the second largest GDPR fine ever imposed.

H&M's GDPR violations involved the "*monitoring of several hundred employees*". After employees took vacation or sick leave, they were required to attend a return-to-work meeting: some of these meetings were recorded and accessible to over 50 H&M managers.

It meant a broad knowledge of their employees' private lives, since personal data included medical records (diagnoses and symptoms of the illness) as well as private details about vacation and family affairs, providing a "detailed profile" used to support the employees' performance evaluation and make decisions about their employment. Some of this knowledge was recorded, digitally stored and partly readable by up to 50 other managers throughout the company. The recordings were sometimes made with a high level of detail and recorded over greater periods of time documenting the development of these issues.

The practice came to light following a data breach in October 2019 when, as a result of an internal error, the data became accessible company-wide for several hours and the press picked up the news making the Commissioner aware of the violation.

Even though details of the decision haven't been published, the Company appeared to have violated the GDPR's principle of data minimization, under which Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (*i.e.*, 'data minimization').

After the Hamburg Commissioner for Data Protection and Freedom of Information was informed about the data collection through press reports, it first ordered the contents of the network drive to be "frozen" and then demanded it to be handed over. The company complied and submitted a data record of around 60 gigabytes for evaluation that confirmed the documented practices.

H&M should have placed strict access controls on the data, and the company should not have used this data to make decisions about people's employment.

As a consequence of the discovery of the violations, H&M management took various corrective measures: apologies and a significant compensation to the employees affected, as well as a newly appointed data protection coordinator, monthly data protection status updates, increasingly communicated whistleblower protection and a consistent concept for dealing with data subjects' rights of access.

The amount of the fine imposed has been considered by experts adequate and also effective to deter other companies from violating the privacy of their employees.

British Airways GDPR fine – €22,046,000

In September 2018, British Airways ("BA") suffered a data breach incident that involved user traffic to the British Airways website being diverted to a fraudulent site where personal information of approximately 400,000 customers and BA personnel was harvested by the attackers.

The Company had inadequate security mechanisms to prevent such cyber-attacks from happening.

The Information Commissioner's Office ("ICO") stated that a "variety of information was compromised by poor security arrangements at the company, including login, payment card, and travel booking details as well name and address information."

The attack was detected only 2 months after it started, in September 2018, due to the aforementioned lack of security measures.

At the time of the breach, British Airways did not have the proper security protocols in place to protect the large amount of personal data it processes and stores.

In July 2019, after a thorough investigation, the ICO issued a notice of its intention to fine British Airways €204.6M or £183.39M for violation of Article 5 (1) f)[23] and Article 32[24] of the GDPR.

According to the ICO's official statement: "*An ICO investigation found the airline was processing a significant amount of personal data without adequate security measures in place. This failure broke data protection law and, subsequently, BA was the subject of a cyber-attack during 2018, which it did not detect for more than two months.*"

ICO expressed concern that the airline failed to detect the breach and was informed by a third party more than two months after the attack.

It was not clear whether or when BA had identified the attack themselves: this was considered to be a severe failing because of the number of people affected and because any potential financial harm could have been more significant.

After that, the ICO and British Airways engaged in negotiations that allowed them to plead their cases regarding the severity of the penalty, which in the end resulted in reduced fine.

On October 16th, 2020, the ICO finally issued a decision to set the fine at £20 million, taking into consideration several reasons:

---

[23] ***Principles relating to processing of personal data*** *- "Personal data shall be: [….] processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')".*

[24] ***Security of processing*** *- "1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate: (a) the pseudonymisation and encryption of personal data; (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; (c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; (d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing. 2. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed. 3. Adherence to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate compliance with the requirements set out in paragraph 1 of this Article. 4. The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by Union or Member State law.*

- BA promptly informing affected data subjects and law enforcement/regulatory agencies;
- a full cooperation with the ICO's enquiries;
- the immediate measures undertaken by BA to mitigate and minimize damage suffered by data subjects (such as the offer to reimburse any financial losses from the theft of card details and the provision of free credit monitoring);
- widespread briefing to journalists and reporting likely to have increased the awareness of other controllers of the risks posed by cyber-attacks and the need to take all appropriate measures to secure personal data;
- the adverse effect to BA's brand and reputation, which will have had some dissuasive effect on BA and other controllers; and
- the impact of the pandemic, both on BA and more generally.

Marriott International GDPR fine – €20,450,000 (£18.4 million)

Marriott estimates that 339 million worldwide guest records (including seven million records related to people in the U.K.) were affected following a cyber-attack in 2014 on Starwood Hotels and Resorts Worldwide Inc. The attack, from an unknown source, remained undetected until September 2018, by which time the company had been acquired by Marriott.

In July 2019, ICO issued an intent to fine Marriott International more than £99 million for infringements of the GDPR. Personal data involved in the breach included guests' names, email addresses, phone numbers, unencrypted passport numbers, arrival/departure information, guests' VIP status and loyalty program membership number. The actor, never identified, installed a code on a device in the Starwood system and through malware gained remote access as a privileged system user which enabled it to infiltrate and take control of their systems.

Marriott notified the ICO and affected individuals in November 2018, some two months after becoming fully aware of the nature of the breach.

According to ICO investigation, there were "failures" by Marriott to put appropriate measures in place to protect the personal data being processed on its systems, as required by GDPR.

On October 30th, 2020, after the related investigation, the Information Commissioner's Office announced its fine of £18.4 million issued to Marriott International, Inc., meaning a significant decrease from the proposed fine of £99 million announced in July 2019.

The Authority considered the steps Marriott took to mitigate the effects of the incident and the economic impact of COVID-19 on their business before setting a final penalty.

According to the data regulator, "*the ICO acknowledges that Marriott acted promptly to contact customers and the ICO. It also acted quickly to mitigate the risk of damage suffered by customers, and has since instigated a number of measures to improve the security of its systems*".

This ICO action came just days after the Authority had hit British Airways with a record-breaking £20 million GDPR fine following a 2018 data breach that affected more than 400,000 of the airline's customers (see previous paragraph), when an investigation by the ICO found that the airline was processing "*a significant amount of personal data without adequate security measures in place*".

Air Europe GDPR fine - €600,000

The Spanish data protection authority ("AEPD") announced, on March 17th, 2021, its decision to fine Air Europa Lineas Aereas S.A. €600,000, following a notification of a security breach regarding unauthorized access to contact details and bank accounts, affecting approximately 489,000 individuals and 1,500,000 data records. In particular, the AEPD outlined that it had imposed a fine of €500,000 on Air Europa for violating Article 32(1) of the GDPR because of its failure to have in place appropriate technical and organizational measures to ensure an adequate level of security, and €100,000 for violating Article 33[25] of the GDPR because it had notified the AEPD of the breach with a delay of 41 days.

The security incident has led to unauthorized access to bank card information, numbering, expiration date and CVV that could have been used to commission fraudulent operations (approximately 4,000 cards were used to commit fraud). Although all those identified were canceled before it is established that there has been any damage to the interested parties.

The AEPD explained that Air Europa was not aware of the existence of the breach until it received a notification from Banco Popular in October 2018. The airline made a first communication to the AEPD a month later and in January 2019 made a full notice about the gap.

According to the aforementioned resolution, Air Europa commissioned a forensic report from IBM in which it is detailed that the "stolen data" included financial and personal data of clients. At the same time, the company also commissioned another

[25] ***Notification of a personal data breach to the supervisory authority*** *- 1. In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay. 2. The processor shall notify the controller without undue delay after becoming aware of a personal data breach. 3. The notification referred to in paragraph 1 shall at least: (a) describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned; (b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained; (c) describe the likely consequences of the personal data breach; (d) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects. 4. Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay. 5. The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with this Article.*

report from Foregenix, a company specializing in security breaches, which identified "*more than 2.7 million unique card numbers that had been extracted from database systems by the attacker*".

The airline indicates that it has only received 20 requests for information from clients derived from the attack and that only three clients stated they had suffered "some type of economic damage".

The APDO concluded that the technical and organizational security measures implemented by the claimed entity were not appropriate to guarantee a level of security appropriate to the risk and prevent unauthorized access to customer data. The volume of records affected amounts to 1.5 million.

The penalty, which in total is 600,000 euros, is divided into two parts: the regulator has fined the airline (i) 500,000 euros for not applying appropriate measures to guarantee data security and, (ii) it added another 100,000 euros for notifying the security breach 41 days late (whilst the law requires that the notification must be, at the latest, 72 hours after having proof of it).

*****

Taking all the above into consideration, the importance of complying with the requirements set out in Articles 32, 33 and 34 GDPR is perfectly clear, due to the cost of non-compliance related to the applicable administrative sanctions.

A data breach (for example, involving sensitive customer information) can be a complicated and critical issue for companies.

The aforementioned cases show how preventing any data loss and fixing the vulnerability should be a priority, ensuring at the same time a prompt data breach notification (what it failed for example regarding Marriot and Air Europe’s breach, but represented a clincher for the reduction of BA’s fine).

Therefore, trying to fly under the radar without any notification and disclosure can lead to negative consequences that only worsen the situation, not only as a result of significant GDPR fines, but also of company's reputation, as well as in terms of risk of claims for damages from data subjects whose data have been viewed as a consequence of a data breach (under article 82 GDPR).

For example, if a cyber attacker illegally accessed the bank accounts of a financial entity’s customers, a law firm could certainly initiate a class action against the company, claiming damages for the problems caused to customers.

V. INTERNATIONAL DATA TRANSFERS AND DATA BREACH

In this section, we address the impact of the GDPR on non-european countries and data breaches in such third countries.

To do so, we first need to take a (now more closer) look at the territorial scope[26] of the GDPR.

Article 3 GDPR defines the territorial scope of the GDPR in three paragraphs.

According to paragraph 1, the application of the GDPR depends on whether the processing of personal data takes place in the context of an activity carried out by an establishment of a controller or a processor in the Union. It does not matter whether the processing takes place in the Union itself.

Paragraph 2 further broadens the scope of application and extends it to data processing operations carried out in the context of offering goods or services in the Union. The extension also covers the monitoring of certain conduct by individuals who engage in that conduct on the territory of the Union.

Paragraph 3 extends the scope of application for processing operations of personal data to places governed by the law of a European Member State by international law.

How should Art. 3 GDPR be understood?

Art. 3 GDPR puts an end to legal uncertainties that have existed in part in the national data protection legislation of the Member States up to now. Until now, it was often up to judges at the national EU level to decide whether data processing operations carried out outside the EU with a clear link to the EU should also be subject to European data protection rules. This is where the regulation now becomes clear. It also subjects to its scope of regulation those operations involving the handling of personal data that are:

- carried out by a branch office.

- carried out by processors outside the EU who specifically offer their goods and services to data subjects in the EU.

- carried out by processors outside the EU for the purpose of profiling data subjects within the European Union.

- carried out by processors outside the EU that are attributable to the Union by virtue of international law.

What are the consequences of Art. 3 GDPR?

Art. 3 GDPR expands the geographical scope of application of the European data protection regulations compared to previously applicable national regulations, in some cases considerably. In the future, companies will not be able to avoid the application of

[26] See above Fn.9

the GDPR by relocating data processing operations to other countries. Since the mere offering of goods and services in the European area opens up the scope of application of the EU General Data Protection Regulation, companies operating internationally must pay particular attention to the required data protection conformity. This also applies, in particular, in view of the significantly increased sanctions framework for data protection violations associated with the GDPR.

But why does this scope pose a threat to globally active companies? To this end, let's take a look at the criteria that must be present for an infringement under the GDPR in this context to third countries (non-EEA country).

a. Data breach and illicit data processings

We should first remind ourselves of the different definitions. As has been explained before the word “data breach” is legally defined in art. 4 (12) GDPR as breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.

And, in comparison - or better, in addition to that - we do have the statutory regulation of art. 5 (1) GDPR, which states, that personal data shall be:

(a) processed lawfully, fairly and in a transparent manner in relation to the data subject (‘lawfulness, fairness and transparency’) and […]

(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures (‘integrity and confidentiality’).

But why do we have to put so much emphasis on that distinction?

Because the outcome is of huge impact. Be reminded that art. 5 (2) GDPR states: “The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 (‘accountability’)”. This means nothing less than the data controller/processor can be held liable for any infringement – any non-compliant behavior – of the GDPR’s principles.

Whereas a data breach according to art. 32, 33, 34 GDPR can lead to various civil court cases for the processor/controller of personal data and huge amounts of indemnifications and compensation claims as well as sanctions according to art. 83 (4) GDPR, illicit data processing according to art. 44 - 49 GDPR leads to civil claims and sanctions according to art. 83 (5) GDPR. And this distinction means nothing more or less, than the fines might get doubled in case of an infringement of Art 44 - 49 GDPR.

And beside this, an illicit data processing can always result in a data breach, because the security measures applied were not sufficient. So the data processor/controller runs a higher risk, which might lead to categorize his behavior, maybe not as intentional, but at least as grossly negligent and therefore be fined higher.

So is it really appropriate to only look at the consequences of a data breach according to the legal definition, or doesn´t it make more sense to evaluate the risks for our group in general and understand the term “data breach” as infringement of the GDPR?

But now let’s have a closer look, why all this is so crucial for international groups.

b. International data transfer

Two far-reaching judgments have been handed down by the European Court of Justice ("ECJ") in recent years, the so-called "Schrems"[27] judgments. Both of those refer to the USA, but please keep in mind, right from the beginning, it's not only the USA we are talking about, but we are speaking about a great number of countries with the same challenge to meet.

What to take into account then?

First we have to understand that every international transfer of data must have a legitimate basis, in accordance with art. 44 - 49 GDPR. In case a legitimate basis is missing, we would process data unlawfully, because we would not follow the statutory requirements of art. 5 GDPR.

Prior to any transfer, a company must generally check whether appropriate data protection guarantees exist in the destination country (Art. 46 GDPR). Exceptionally, however, such an individual check is not required if the EU Commission has adopted an adequacy decision for the relevant destination country (Art. 45 GDPR). Such an adequacy decision for the USA was the Privacy Shield[28] (EU 2016/1250). With this Privacy Shield, the EU Commission had determined that the USA has a data protection system that is comparable to that of the EU.

However, the ECJ overturned this Privacy Shield in the summer of 2020[29] in the aforementioned Schrems II decision with immediate effect. Reason for this: under U.S. law, the largely comprehensive collection of personal data by security authorities is possible without appropriate data protection safeguards for EU citizens. The rights of the U.S. authorities to intervene are too comprehensive and disproportionate to be considered comparable with the guarantees of European law. Thus, according to the ECJ, the level of protection in the U.S. can no longer be considered adequate.

As a consequence, programs and applications that transfer personal data to the USA can no longer be used in a legally compliant manner without further thinking. The transfer of data to the USA without carrying out an adequacy check in the individual case thus violates the GDPR, the ECJ informs us. Since every application constantly carries out such data transfers in the background, the strict interpretation is that the mere use of the data violates the GDPR.

In one fell swoop, the ECJ has thus turned the entire transatlantic data transfer on its head. Although the ruling was not unexpected, it still poses a number of problems for data controllers. After all, which service and which tool installed on a work computer does not transmit data to the U.S.A.? What is still allowed to be used then?

First of all, it is important to note that the transmission - *i.e.* the mere sending to the third country - is already data processing (step 1). This means that the transfer itself, regardless of the subsequent further processing (*e.g.*, in the case of the U.S.A., access by a U.S.A. security authority (step 2), requires a legal basis in the GDPR.

---

[27] Maximilian Schrems is an Austrian lawyer, author and privacy activist https://de.wikipedia.org/wiki/Max_Schrems

[28] ECJ ruling C-362/14

[29] ECJ ruling C-311/18

For most companies, the following legal bases are practically relevant for data transfers to third countries:

- Adequacy Decision (45 GDPR).
- Appropriate safeguards (Art. 46, 47 DSGVO)
- Exceptional situations (49 GDPR).

It has already been elaborated above that after the ECJ ruling in the Schrems II case, there is no longer an adequacy decision, the Privacy Shield simply no longer exists. Article 45 is therefore no longer a possible legal basis. This leaves the appropriate safeguards and Article 49 GDPR for a legal data transfer to the USA. This is the only way to avoid an infringement under the GDPR.

Art. 49 GDPR lists some constellations in which personal data may be transferred to insecure third countries without an adequacy decision by the Commission (Art. 45) or appropriate safeguards (Art. 46, 47).

According to art. 49, a transfer is permitted if this transfer is necessary for important reasons of public interest. And it is precisely this standard that, in the view of the U.S. Department of Commerce, is suitable as a legal basis for the transatlantic transfer of data. The U.S. Department of Commerce is of the opinion that the prevention of cyber attacks and the prevention of criminal acts as well as the collection of intelligence for counter-terrorism and attack prevention is also in the public interest of the EU and is therefore covered by Art. 49 (1) (d) GDPR.

However, there are doubts about this opinion, because it is not that simple: <u>different processing operations require different legal bases according to the GDPR.</u>

We need to distinguish the transfer of data to the U.S.A. and the granting of access in the U.S.A. Both are different processing operations, each requiring an independent legal basis. From the company's point of view, a solution is needed that provides a legal basis at least for the first step (transfer to the U.S.A.), regardless of whether or how step 2 (granting access) is still carried out. If, on the other hand, the legal basis for step 1 were to depend on step 2, the solution would be practically unusable for companies. This is because it would then only work if step 2 actually exists.

Was that understandable? Probably not...

Again, the problem from the ECJ's point of view is that the U.S.A. security authorities have far-reaching powers to access personal data. For justification, the judgment refers to FISA 702 and EO 12333. In the same breath as these two laws, the CLOUD Act is regularly mentioned in public. Three american legal acts therefore determine the access of the U.S.A. authorities to personal data.

But let's not forget, the aforementioned paragraph is step 2 (granting access), not step 1 (transferring data)!

The U.S.A. government is convinced that these aforementioned legal beacons provide a level of protection comparable to that of the EU. Thus, a transfer of personal data would not be a problem according to Schrems II.

But is this view of the U.S.A. Department of Commerce relevant for us Europeans?

The answer is simple: **NO!**

Because for us, the following applies**: there is an infringement as long as there is no legal basis for the data transfer according to GDPR. And if anybody gets unauthorized access to that data it is a data breach according to GDPR.**

Does that mean we are constantly and continuously in breach of the GDPR, because U.S.A. authorities have access to our personal data?

Or can we still derive a legal basis for a legal data transfer from Art. 49 GDPR - and thus no violation of the GDPR occures?

However, Art. 49 GDPR is an exception to the principle that data transfer to unsafe third countries is prohibited. A scheduled and regular data transfer cannot be derived from it.

According to Art. 49 GDPR, the transfer of personal data to unsafe third countries needs a corresponding standardized reason. Reasons for exceptionally permissible transfers include[30]:

Consent: If we transfer data on the basis of consent, this consent must be given by the data subject in full knowledge of the facts. This means that we must inform our employee/customer about the specific risks of a transfer to the USA. In addition, the other requirements for effective consent must also be met. General information on data processing is definitely not enough. Without a corresponding detailed explanation, consent will not work.

- Fulfillment of a contract: according to the EDPB transfers on the grouds for the performance of a contract should only be “occasionally”. Corporate processes and business structures cannot be aligned with an “occasional” possible business data transfer.
- Important reasons of public interest: although this exception is not limited to occasional transfers, it does not justify systematic transfers on a large scale. Companies would therefore have to check before each data transfer whether it is absolutely necessary.
- Assertion, exercise or defense of legal claims: this as well means an individual check for each transfer.
- Protection of vital interests of natural persons: this means according to the beforementioned the need to check individually.

But we are not looking for reasons or a legal base for exceptional data transfers but for standardized regular data transfers, so no legal base can be found for that in art. 49 GDPR.

If we cannot fall back on either Art 45 or Art 49 of the GDPR, would it be possible to use a legal basis from Art 46 GDPR?

[30] FAQ-Catalogue of EDPB for ECJ ruling C-311/18:
https://edpb.europa.eu/sites/default/files/files/file1/20200724_edpb_faqoncjeuc31118_de.pdf

For this purpose, the EDPB has issued a recommendation[31], which consists of 6 main steps:

1. Do we know our data transfers?
2. Legal basis for transfer
3. Investigate the practical effectiveness
4. Take appropriate protection measures
5. Implementation
6. Monitoring

With these 6 steps we would arrive at a legal data transfer and thus a prevention of infringements for all data transfers to third countries that are not subject to an adequacy decision.

First checkpoint: Do we know our data transfers?

The question about the knowledge of our data transfers is quickly answered when we have access to a directory of administrative activities (Art. 30 GDPR), which involves a lot of internal work. This directory is worth its weight in gold. Because on the basis of the recorded activities, the appropriateness of the purpose of the transfer as well as the necessary level of processing can be addressed again (Art. 5 GDPR). And this must theoretically be done individually each time before each transfer. And the worst thing is, each storage process in a cloud is already a data transfer in the sense of the GDPR. What is the extent....?

Keep in mind: if we do not carry out an individual check, we act illicit!

Second checkpoint: legal basis

Art. 46 GDPR mentions the following safeguards:

- Standard Data Protection Clauses
- Binding Corporate Rules (BRC)
- Codes of Conduct
- Certification mechanisms.

Standard data protection clauses were not rejected by the ECJ in the Schrems II ruling and can in principle serve as a legal basis. Especially, of course, between two companies that are party to a contract. Third parties cannot, of course, be bound by such standard data protection clauses.

---

31 https://edpb.europa.eu/sites/edpb/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_en.pdf

As it could not be more up to date, the European Commission has just published[32] on June 4th, 2021[33] an implementing decision (2021/3701/EC) on new standard contractual clauses. Until that just recent date there were no standard contractual clauses yet recommended by the EU Commission. In the annex to this decision they have provided standard contractual clauses[34] that can be used as legal base according to art. 46.

EU companies have 18 months of a transition period to implement these newly recommended standard contractual clauses to our agreements.

But standard contractual clauses and other transfer tools mentioned under Article 46 GDPR do not operate in a vacuum. The Court as well as the commission now state that controllers or processors, acting as exporters, are responsible for verifying, on a case-by-case basis and, where appropriate, in collaboration with the importer in the third country, if the law or practice of the third country impinges on the effectiveness of the appropriate safeguards contained in the Article 46 GDPR transfer tools[35].

This means tha companies have the following target to meet: Install the recommended standard contractual clauses and use reinforcing additional security measures to meet the level of protection needed.

However, it gets more difficult with the next checkpoint to comply with to act accordingly to art. 46. What do we say about practical effectiveness?

But what does this question mean? It is to assess whether the legal situation and legal reality in the third country do not undermine the level of data protection contractually agreed in the standard data protection clauses. But how do you do that? One evaluates the case law in the third country on this, one pays attention to the opinions of the bodies (Council of Europe, UN bodies, etc.).

It doesn't sound bad, but it is: because simple is different. The answer to this point requires a lot of effort. There were recommendations from the EDPB on this as well.[36]

Please remember: **if not successfully completed, then non-compliant to GDPR!**

The fourth checkpoint concerns the adoption of appropriate protective measures.

---

[32] https://ec.europa.eu/commission/presscorner/detail/en/IP_21_2847

[33] decision 2021/3701/EC: https://ec.europa.eu/info/sites/default/files/1_en_act_part1_v5.pdf

[34] Standard contractual clauses for controllers and processors: https://ec.europa.eu/info/law/law-topic/data-protection/publications/standard-contractual-clauses-controllers-and-processors
Standard contractual clauses for international transfers: https://ec.europa.eu/info/law/law-topic/data-protection/publications/standard-contractual-clauses-international-transfers

[35] See footnote no. 34:
https://edpb.europa.eu/sites/default/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_en.pdf

36

https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_recommendations_202002_europeanessentialguaranteessurveillance_en.pdf

For the exchange with the USA, it is now clear that additional technical protection mechanisms must be built in to the standard contractual clauses to prevent access to the data by U.S.A. security authorities. In its Annex 2, the EDPB has already listed some examples[37]:

- Data storage for backup and other purposes do not require access to data in the clear
- Transfer of pseudonymised data
- Encrypted data merely transiting third countries
- Protected recipient
- Split or multi-party processing
- Transfer to cloud services providers which require access to data in the clear
- Remote access to data for business purposes
- Additional contractual measures
- Providing for contractual obligations to use specific technical measures
- Transperancy obligations
- Obligations to take specific actions
- Empowering data subjects to exercise their rights
- Organisational measures
- Internal policies for governance of transfers especially with groups of eterprises
- Transperancy and accountability measures
- Data minimization measures
- Adoption of standards and best practices
- Others

If the review leads to the conclusion that an adequate level of protection cannot be ensured in the destination country even with the adoption of additional technical security measures, all processing operations should be terminated and the data records deleted in the third country.

If one stubbornly adheres to the publications of the EDPB and considers them to be correct, then this should be the end of the line for data transfers to the USA at the latest. It is unlikely that technical measures will (can) be taken that meet the requirements of the ECJ and the EDPB. This is because, regardless of the risk involved in the transfer, legal opinions are being expressed on the part of the supervisory authorities that push the necessary measures to astronomical heights.

---

37 https://edpb.europa.eu/sites/default/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_en.pdf

The 5th point is a piece of cake, provided that point 4 is positively examined, because then one "only" has to implement these technical measures. Of course, the supervisory authorities should be involved so that there is no rude awakening later.

And finally, you have to monitor everything that has been done so far in step 6 and (of course) repeat these checks on an ongoing basis.

So far so good, let's assume we haven't committed an infringement up to this point. But what if something goes wrong?

Good question.....

The only sure thing seems to be that without an adequacy decision by the Commission, it depends on the individual case and individually on each transfer. And that each individual case - *i.e.*, each data transfer to third countries such as the USA - is subject to such an assessment.

The paper is very clear about who is to carry out this review and assessment: the controller, i.e. the data transferring company. This is because it is responsible for the legality of its transfer plans and also bears the risk of making the wrong decision. This is also clear from Art. 5 II GDPR, which lays down the cornerstone of responsibility and (above all) liability.

In the event of wrong decisions and false assessments, the company must answer. The supervisory authority can take regulatory measures, for example, prohibit data transfers or order a fine. To minimize this risk, clean and careful documentation of these six steps is extremely important. This is also the responsibility of the person in charge: He must be able to prove to the supervisory authority upon request that his processing (including the transfer) is lawful and that he has checked this cleanly and carefully.

Only in this way can a sanction be avoided or mitigated.

It is also difficult that the ECJ has not granted a grace period or transitional period. Ultimately, this probably means that almost every transfer of personal data to the U.S.A. currently violates the GDPR.

It should be clear that this assessment serves no one. Neither the companies, nor the data subjects, nor the data protection authorities, nor the supervisory authorities. In any case, there is a pressing need for long-term solutions and short-term measures to end this unspeakable condition. Ultimately, this cries out for a new adequacy decision!

But as long as we don't have one, we should stick to the guidelines of the European Data Protection Supervisor.[38] And implement immediately the newly recommended standard protection clauses with the additional security measures on top.

While it will not finally lead us to legal certainty in respect of the US, it appears to be a first step in the direction of the ECJ, so that the intention of the judgment can at least be taken up and pursued. Whereas with the newly published decision of the Commission about those standard protection clauses at least we have a GDPR-compliant path to follow now… For sure until the next ruling of the ECJ!

The risk-based approach of the GDPR will be followed in a two-stage plan. The first stage is to identify the particularly high-risk transfers. These are those where individuals

[38] https://edps.europa.eu/sites/edp/files/publication/2020-10-29_edps_strategy_schremsii_en_0.pdf.

face a particularly high risk in the transfer. This is because anything that could reflect negatively on the individual must be protected immediately.

In the second stage, all transmissions are then to be investigated so that appropriate measures can then be taken adequately.

A mapping is therefore absolutely necessary. Based on this, it is then possible to divide the data into (i) high-risk transfers and those without a legal basis pursuant to Art. 46 GDPR, as opposed to (ii) the others. For the first group, there is a compelling need for action and the logical decision is not to carry out any new transfers without prior checks, including the corresponding assessment documentation (see above for 6 steps).

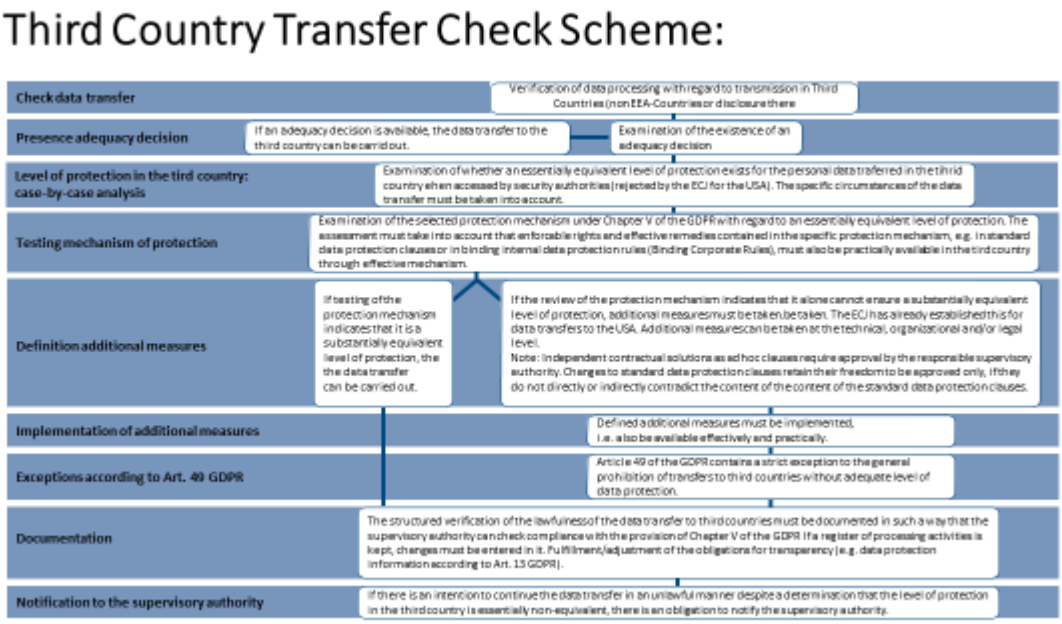
For transfers of the second group, the installation of a Transfer Impact Assessment (TIA) applies in the medium term, where the level of data protection in the respective third country is evaluated. On the basis of this, a decision can then be made as to whether transfers should continue.

So what does all this mean for us now?

The supervisory authorities are clearly currently of the opinion that a legal transfer of personal data to the U.S.A. is possible at best with a lot of effort and only in some cases. The only completely legal way possible without loss of time is to stop all dara transfers to the U.S.A.

But please let’s not stick only to the U.S.A. What has been stated above applies to all non-european countries that have not yet been declared as a country with adequate protection level (Art. 45 GDPR).

Data breaches, illicit data processing and further actions violating the GDPR regulations are likely taking place right this moment, worldwide, are and should stay on the agenda and affect us in our group!



39

c. cross-border breaches

Now, let's take a look at the next question: What do we do if a data breach (according to the legal definition)[40] has occurred in a third country? Maybe someone gets access to personal data of an EU citizen?

Well, the answer is quite simple: Art. 33 GDPR applies. We have to notify the supervisory authority.

But which one? Aren't there more than one in the EU? The answer to that question is Art. 56 GDPR: it's the supervisory authority of the main establishment that is competent as lead supervisory authority for cross-border processing. And the lead supervisory authority is the sole interlocutor.

This means that whenever a breach takes place in the context of cross-border processing and notification is required, the controller will need to notify the lead supervisory authority. Therefore, when drafting its breach response plan, a controller must make an assessment which supervisory authority is the lead supervisory authority that will need to be notified. This will allow the controller to respond promptly to a breach and to meet its obligations in respect of Article 33. It should be clear that in the event of a breach involving cross-border processing, notification must be made to the lead supervisory authority, which is not necessarily where the affected data subjects are located, or indeed where the breach has taken place. When notifying the lead authority,

---

[39] Federal Commissioner for Data Protection and Freedom of Information, Germany

[40] „data breach" is legally defined in art. 4 (12) GDPR as breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed

the controller should indicate, where appropriate, whether the breach involves establishments located in other Member States, and in which Member States data subjects are likely to have been affected by the breach. If the controller has any doubt as to the identity of the lead supervisory authority then it should, at a minimum, notify the local supervisory authority where the breach has taken place.

To make it simple: It does not make any difference where the data breach occurs. Notifictation to the supervisory authority is mandatory. **The same rules apply for all cases!**

VI. CONCLUSIONS

The liability model of EU data protection law is consistent with the Principles of European Tort Law, provided one takes into account the "general" liability of controllers and the "proportional" liability of processors.

In many ways, the GDPR merely constitute a codification of general tort law principle that the controller carries "general" (or "primary") liability exposure for any processing activity under its control. It also recognizes that processors should be directly liable towards data subjects. The result is a cumulative liability regime, in which the data subject has a choice whether to sue the controller, the processor, or both – at least in cases where both controller and processor are at least partially responsible for the damage.

However, as a globally active group, how do we treat those obligations that come along with this liability regime – to be compliant and at the same time - still pursuing our business?

This leads us to the ultimate question: Is the GDPR stating obligations of means or obligations of results? Moreover, how do we answer that question?

Because a current prevailing opinion on this question is still pending and most probably will always be pending due to changes in opinions not only of the ECJ or the data protection authorities, but maybe as well due to our own experiences.

From our own experience with data breaches within Enel group, we conclude that the GDPR is to be treated as obligation of means. Why that?

The risk of data breaches or infringements cannot be reduced to null; it will always exist and most probably, it will be realized at one point or another. So the only solution is to be compliant by means of implementation of necessary and reasonable security measures on top of all kind of data protection precautions and internal company rules, standard contract rules as well as providing information towards clients and business partners and – last, but not least – the repeated checks and double-checks and evaluations and re-evaluations of all those measures. As long as we follow that path, be compliant by any possible measures – until now - we were spared from being fined, because we could proof that we have implemented everything there is available and reasonable to protect the personal data and the data subjects from being exposed.

As long as the EDPB (or ECJ) is not of the opinion that the GDPR is setting obligations of result, we should be firm on our current approach and follow it through. Because we

were proven right so far, not only but also mainly because it is the only reasonable way to still be active in business and not be paralyzed by anxiety of sanctions.

BIBLIOGRAPHY

- https://www.privacy-ticker.com/gdpr-fines-and-data-breach-reports-increased-in-2020/
- https://www.dlapiper.com/en/belgium/insights/events/2021/01/dla-piper-gdpr-fines-and-data-breach-survey/21-jan-2021/
- Three years of GDPR: the biggest fines so far - BBC News
- www.bfdi.bund.de: Websites of BfDI - Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit/Informations provided by: Federal Commissioner for Data Protection and Freedom of Information, Germany
- https://eur-lex.europa.eu/legal-content, Recitals of GDPR
- Der Datenschutzkommentar, Bergmann/Möhrle/Herb, Juni 2021, 62. Ergänzungslieferung
- www. techlawgermany.net, Natalie Dessauer, Blog 27.04.2018, Der räumliche Anwendungsbereich der Datenschutzgrundverordnung und ihre Auswirkungen auf Unternehmen außerhalb der EU
- www. Privacyshield.gov; Processing guidance, FAQs -EU-U.S. Privacy Shield Program Update, last update 31.03.2021
- https://www.europarl.europa.eu/RegData/etudes/ATAG/2020/652073/EPRS_ATA(2020)652073_EN.pdf
- https://de.wikipedia.org/wiki/Max_Schrems
- FAQ-Catalogue of EDPB for ECJ ruling C-311/18: https://edpb.europa.eu/sites/default/files/files/file1/20200724_edpb_faqoncjeuc31118_de.pdf
- https://edpb.europa.eu/sites/edpb/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_en.pdf
- https://ec.europa.eu/commission/presscorner/detail/en/IP_21_2847
- decision 2021/3701/EC: https://ec.europa.eu/info/sites/default/files/1_en_act_part1_v5.pdf
- Standard contractual clauses for controllers and processors: https://ec.europa.eu/info/law/law-topic/data-protection/publications/standard-contractual-clauses-controllers-and-processors
- Standard contractual clauses for international transfers: https://ec.europa.eu/info/law/law-topic/data-protection/publications/standard-contractual-clauses-international-transfers

- https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_recommendations_202002_europeanessentialguaranteessurveillance_en.pdf
- https://edps.europa.eu/sites/edp/files/publication/2020-10-29_edps_strategy_schremsii_en_0.pdf.
- https://www.doag.org/de/home/news/dsgvo-vs-cloud-act/detail/
- https://www.delegedata.de/2020/10/schrems-ii-us-cloud-act-kein-problem-zumindest-nach-ansicht-der-landesregierung-nrw/
- http://www.oraworld.org/fileadmin/documents/21-ORAWORLD.pdf#page=7
- http://www.oraworld.org/fileadmin/documents/22-ORAWORLD.pdf#page=17
- Article 29 Data Protection Working Party – Guidelines on Personal data breach notification under Regulation 2016/679 Adopted on 3 October 2017 as last revised and adopted on 6 February 2018
- Article 29 Data Protection Working Party – Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679 as adopted on 4 April 2017
- European Data Protection Board - Guidelines on Examples regarding Data Breach Notification Adopted on 14 January 2021, Version 1.0
- Agencia Espanola de Proteccion de Datos – Guide on personal data breach management and notification, May 2021: https://www.aepd.es/sites/default/files/2019-09/Guide-on-personal-data-breach.pdf
- European Union Agency for Cybersecurity – Recommendations for a methodology of the assessment of severity of personal data breaches: https://www.enisa.europa.eu/publications/dbn-severity
- Commission Implementing Decision (EU) 2021/915 of 4 June 2021 on standard contractual clauses between controllers and processors under Article 28(7) of Regulation (EU) 2016/679 of the European Parliament and of the Council and Article 29(7) of Regulation (EU) 2018/1725 of the European Parliament and of the Council C/2021/3701, OJ L 199, 7.6.2021, p. 18–30
- Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council C/2021/3972, OJ L 199, 7.6.2021, p. 31–61
- Deloitte AG – 'GDPR Top Ten, #9: Security and breach notification': https://www2.deloitte.com/ch/en/pages/risk/articles/gdpr-security-and-breach-notification.html
- https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations_en

- https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/
- https://edps.europa.eu/data-protection/our-role-supervisor/personal-data-breach_en
- Article 29 Working Party – 'Opinion 4/2007 on the concept of personal data' as adopted on 20 June 2007
- Schwartz PM and Solove DJ – 'The PII Problem: Privacy and a New Concept of Personally Identifiable Information', New York University Law Review Volume 86, Number 6 (2011): https://www.nyulawreview.org/issues/volume-86-number-6/the-pii-problem-privacy-and-a-new-concept-of-personally-identifiable-information/
- Article 29 Working Party – 'Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679' as adopted on 3 October 2017
- British Court of Appeal Ruling of 2 October 2019: https://www.judiciary.uk/wp-content/uploads/2019/10/Google.finaldraftjudgment. approved-2-10-19.pdf
- Linklaters – 'Data breaches under the GDPR: Five key questions': https://www.linklaters.com/en/insights/blogs/digilinks/data-breaches-under-the-gdpr-five-key-questions
- Thomson Reuters Practical Law – Data Protection: https://uk.practicallaw.thomsonreuters.com/Browse/Home/Practice/DataProtection?transitionType=Default&contextData=(sc.Default)&comp=pluk&firstPage=true
- https://www.lexology.com/library/detail.aspx?g=4357ef0b-78f4-401d-b660-faf262dc56f7
- https://www.metacompliance.com/blog/5-damaging-consequences-of-a-data-breach/
- Bristows – 'UK: Class Actions – Scarier Than A GDPR Fine?': https://www.mondaq.com/uk/trials-appeals-compensation/1027854/class-actions-scarier-than-a-gdpr-fine-
- https://ico.org.uk/your-data-matters/data-protection-and-journalism/taking-your-case-to-court-and-claiming-compensation/
- Loyens and Loeff – 'Quoted', Edition 133, June 2020: https://www.loyensloeff.com/media/478464/quoted-133.pdf