SIGN UP

PANGEANET

INTERNATIONAL NETWORK OF INDEPENDANT LAW FIRMS

VISIT OUR WEBSITE

NEWSLETTER 6

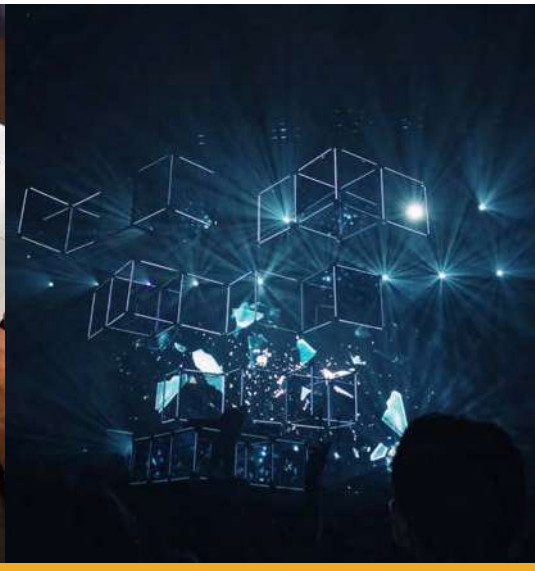
January 2024

DATA, INFORMATION & CYBER LAW

PangeaNet is an association of independent law firms from over 23 countries forming an international law firm network. The Pangea Practice Group for Data, Information and Cyber Law (DICL) consists of experts in IT, data protection law, privacy, cybersecurity and open data issues. We support your digital transformation and guide you in the protection, use and defence of your immaterial assets from a legal perspective.

A multi-jurisdictional experts approach

A group of specialists familiar with their respective local laws and customs

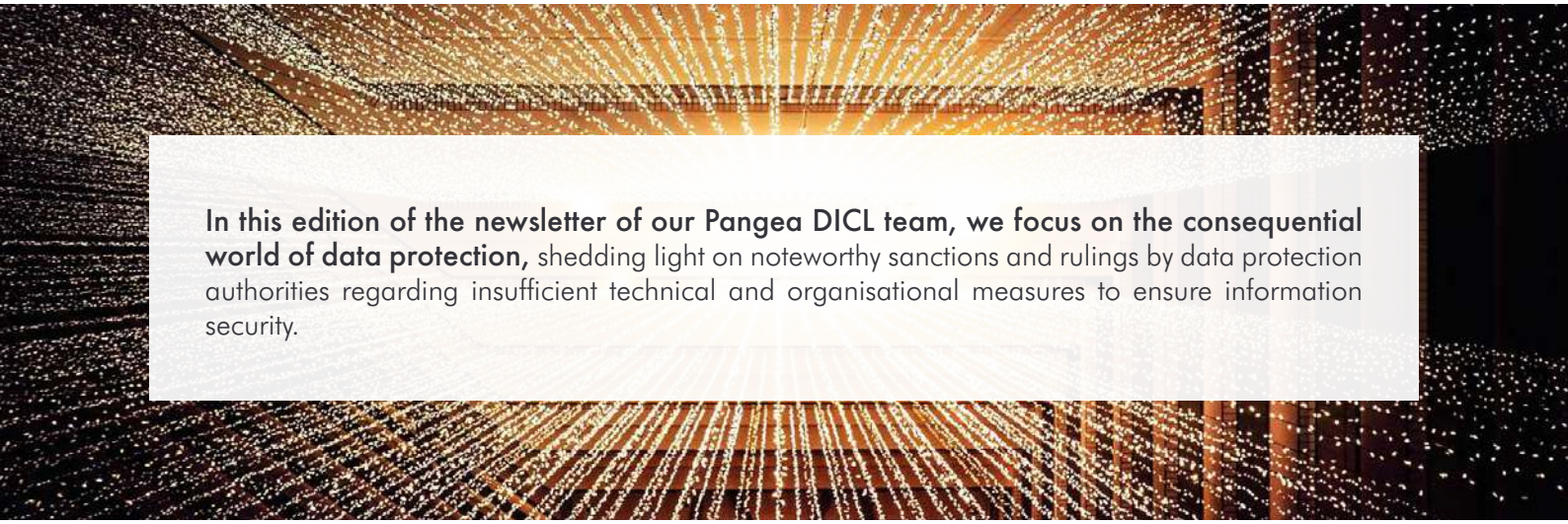


A real curiosity and appetite for the latest technological developments & phenomena

EDITORIAL

THE NUMBER OF DATA BREACHES CONTINUED TO RISE DRAMATICALLY IN 2023, MORE AND MORE COMPANIES ARE PLACING CYBERSECURITY AT THE TOP OF THEIR PRIORITY LIST

In 2023, the average cost of a data breach has reached a record high (once more). In addition to those costs and reputational damage, companies should also be wary of the penalties that can be imposed.



In this edition of the newsletter of our Pangea DICL team, we focus on the consequential world of data protection, shedding light on noteworthy sanctions and rulings by data protection authorities regarding insufficient technical and organisational measures to ensure information security.

Other relevant and related topics are also discussed. Here's a glimpse into the insightful articles featured in this issue:

- **Italian Authority Takes Decisive Action** - Marta Margiocco opens the discourse by examining the Italian data protection authority's sanctions against Benetton for personal data processing related to marketing and profiling purposes. Her analysis serves as a compelling case study, underlining the repercussions of inadequate safeguards.

- **Consequences for a Belgian Telecom Provider** - Michiel Beutels shares a DPA decision where a telecom provider was penalised 20,000 EUR for a data breach and the failure to implement sufficient technical and organizational measures. The decision serves as a stark reminder of the tangible consequences organisations face for lapses in data security.

- **Swiss rules on White Hat Hackers** - Julia Bhend navigates the regulatory landscape surrounding "white hat hackers" under Swiss law, offering insights into the legal frameworks governing ethical hackers.

- **Compensation in Germany: A Closer Look** - Sebastian Meyer delves into the compensation landscape for data protection incidents in Germany. His contribution underscores the growing significance of accountability and restitution in the aftermath of (for instance) data breaches.

- **AI Deployment: Critical Questions** - Richard Nicholas provides a comprehensive guide with "Eight questions to ask before you use AI in your organization". His insights extend beyond the allure of AI, offering a good framework for AI deployment amid the evolving data protection landscape.

- **India's Data Protection Law** - Rahul Khosla marks the dawn of a new era in India with the enactment of its first ever Personal Data Protection Law. His exploration unveils the key implications and transformative aspects of this landmark legislation for data protection in India.

- **Navigating EU-U.S. Data Transfers** - Tomáš Mudra explores the challenges and potential solutions for EU-U.S. data transfers, pondering whether the Data Privacy Framework could be the guiding light at the end of the tunnel. His insights offer clarity on the evolving landscape of international data protection.

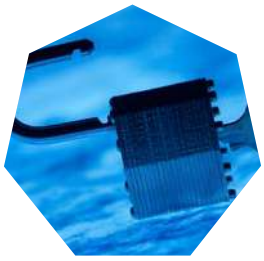
- **Joint Protection for Whistleblowers and Personal Data** - Matthieu Bourgeois and Laurent Badiane emphasize the indispensable need for joint protection concerning whistleblowers and personal data. Their contribution explores the complexities of safeguarding individuals and their sensitive information in a dynamic information environment.

Michiel Beutels
Litiguard Law Firm, Belgium
mb@litiguard.eu

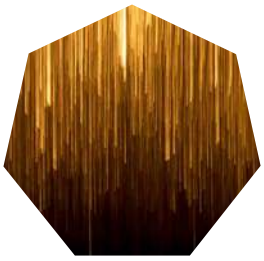
Index

France - Whistleblowers and personal data: joint protection is essential! 6

Belgium - Belgian telecom provider penalised 20k€ for data breach and failure to implement sufficient technical and organisational measures 7



Switzerland - "White hat hackers" – Regulation under Swiss Law 9

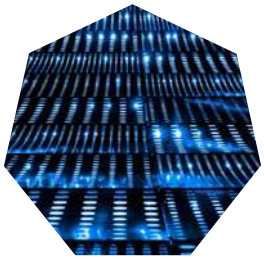


India - A dawn of a new era in India: India's First Ever Personal Data Protection Law 12

The United Kingdom - Eight questions to ask before you use AI in your organisation - and an answer to the question "is this OK?..." 15

Italy - Personal data processing for marketing and profiling purposes: the Italian data protection authority sanctions Benetton. 16

Index



Czech Republic - For EU-U.S. data transfers, is Data Privacy Framework the light at the end of the tunnel? | 18

Germany - Compensation for data protection incidents in Germany | 19

• FRANCE

Whistleblowers and personal data: joint protection is essential!

In this article, we provide a general overview of the whistleblowing legal framework.

A relatively recent regulation, in response to US sanctions.

Michel Sapin (who was, at the time, France's Minister of Economy and Finance) initiated the law "relating to transparency, the fight against corruption and the modernisation of economic life" (known as the "Sapin 2 law", enacted on 9 December 2016, n° 2016-1691). He acknowledges that such law was intended to "bring France up to the best international standards in the field of transparency, and in action against corruption" (press release published on 31 March 2016, by the Government Information Service). This initiative, preceded by law n° 2013-1117 of 6 December 1993 (which strengthened the legal framework governing economic, financial and tax crime), was - as we know - motivated by the desire to correct France's poor ratings in the fight against corruption and to dampen the desire of foreign jurisdictions to punish French companies that fail in this area by means of repressive legislation with extraterritorial scope (as was the case, for example, with Alstom, which was fined more than 770 000 000 dollars by the US Courts for acts of corruption).

Whistleblowers: extensive protection.

While most of its provisions apply to a limited series of financial offences (corruption, influence peddling, illegal interest-taking, etc.), the Sapin 2 law enacted from the outset a protective regime for all those who take the risk, selflessly and in good faith, of revealing facts constituting violations of a standard of domestic (legislative or regulatory), Community or international law (and ratified or approved by France), whatever its nature, provided that it threatens the public interest. Initially confined to "serious and manifest" breaches of the law and to facts directly witnessed by the whistleblower, this protection was then extended to all breaches, including those reported to the whistleblower, by the "Waserman" law (n° 2022-401 of 21 March 2022), which also extended protection to non-profit "facilitators" (trade unions, associations, etc.) and to persons "in contact" with a whistleblower (relatives, colleagues, etc.). In addition, the previous prioritisation (imposing that the whistleblower should first use internal channels, then, in the event of inaction, external channels – the courts, ombudsman, etc. - and, lastly, public channels) has been made more flexible by giving the whistleblower the freedom to choose between internal or external reporting.

Protection of data relating to whistleblowers: the CNIL's vigilance is the essential tool in this area.

The protection afforded to whistleblowers, which in particular guarantees them strict confidentiality (with regard to their identity and that of the persons and facts cited in the report), also implies protection

of the data relating to them. In order to guide organisations (both those subject to the Sapin 2 law or other regulations requiring them to set up whistleblowing systems, as well as those that are not subject thereto but nevertheless wish to do so) in complying with the GDPR to protect such data, the CNIL adopted a set of guidelines on 18 July 2019, a new version of which has just been published on 23 July 2023. The updated guidelines will need to be looked at for any further compliance aspects to be taken into account. These guidelines include the need to inform data subjects, limit data retention periods and carry out a data protection impact assessment (DPIA). To comply with these requirements, the adoption of a software tool will be a crucial asset, particularly for companies with multiple geographical locations.


Laurent Badiane & Matthieu Bourgeois
In charge of the Intellectual Property and Digital Law Team
Partners, klein • wenner

BELGIUM •

Belgian telecom provider penalised 20.000,00 EUR for data breach and failure to implement sufficient technical and organisational measures

In a recent case, a telecommunications provider has been penalised with a 20.000,00 EUR fine by the Belgian data protection authority (GBA / APD) for a data breach and failure to implement effective security measures.[1] This article delves into the details of the case, highlighting the key elements of the decision made by the Belgian DPA.

The incident in question involved a telecommunications provider that – as a data controller – had assigned a customer's phone number to another individual for a duration of four days. During this period, the data subject's SIM card was deactivated, leading to a significant breach of the customer's privacy. Notably, this breach exposed the data subject's personal calls, communication data,

[1] *Geschillenkamer GBA, beslissing ten gronde 101/2022 van 3 juni 2022*

and linked accounts to an unauthorized third party. Moreover, the third party gained access to the data subject's SIM card number, increasing the severity of the breach.

The Belgian DPA presented several allegations against the controller. Firstly, it contended that the controller failed to implement the necessary technical and organisational measures to prevent such a data breach. Secondly, the controller was accused of conducting an incomplete and potentially incorrect identity verification of the third party before assigning the phone number to that third party. Lastly, the controller was charged with not notifying either the data subject or the DPA about the data breach.

> THE BELGIAN DPA IMPOSED A 20.000,00 EUR FINE ON THE TELECOMMUNICATIONS PROVIDER FOR THE DATA BREACH AND ITS FAILURE TO IMPLEMENT SUFFICIENT TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE INFORMATION SECURITY.

In response to these allegations, the controller argued that it could not collect identification data when switching subscriptions due to a purported commercial purpose. Instead, they requested a phone and SIM card number for identity verification. The controller also asserted that they had adequate technical and organisational measures in place to safeguard the data. Furthermore, the controller claimed that the impact on the data subject's personal life was minimal, as most applications had two-step verification enabled. They also argued that there was no obligation to notify the data breach to the DPA, as it was a single, short-lived incident without sensitive data involvement.

The Belgian DPA rejected the controller's argument concerning a commercial purpose when selling post-paid subscriptions. According to the DPA, the primary goal of identity verification is to detect and prevent fraud, including unauthorized use of phone numbers. The DPA contended that a proper identity verification process would have prevented the data breach.

Additionally, the DPA found the controller's technical and organisational measures to be insufficient, rejecting the argument that the data breach had minimal impact on the data subject's personal life. The DPA emphasised that two-step verification did not prevent access to personal data by someone in possession of the phone number. Furthermore, they highlighted the high risk associated with telecommunication data, citing the Digital Rights Ireland case[2] and the potential misuse of SMS for impersonation and personal data access.

As a result, the DPA concluded that the controller violated various articles of the GDPR due to inadequate identity verification and insufficient security measures. Regarding the lack of notification, the DPA asserted that it was indeed necessary, emphasising that the risk remained high for the data subject. The potential

[2] *ECJ 8 April 2014, C 293/12 and C 594/12*

damages from the usage of a phone number included discrimination, identity theft, fraud, financial loss, and damage to the individual's reputation. The DPA also pointed out that SMS data might contain special categories of personal data.

In conclusion, the Belgian DPA imposed a 20.000,00 EUR fine on the telecommunications provider for the data breach and its failure to implement sufficient technical and organisational measures to ensure information security. This case underscores the importance of robust security practices and the serious consequences that can result from data breaches and inadequate identity verification procedures.

If you would have any questions regarding this topic, do not hesitate to contact us.

Michiel Beutels
Litiguard Law Firm

"White hat hackers" – Regulation under Swiss Law

White hat hackers are ethical hackers working to detect vulnerabilities in the system in a helpful way. Unlike "black hat hackers[1]", who seek to exploit them for gain or use them to benefit a particular cause, white hat hackers penetrate the system to locate the vulnerabilities and provide solutions to fix them to ensure safety. Recently, so called "white hat hackers" have increasingly reported data protection and security breaches to the Swiss Federal Data Protection and Information Commissioner (FDPIC). The FDPIC has therefore published a factsheet for ethical hackers[2].

Legal situation under the Data Protection Act
While white hat hackers operate with noble intentions, they are not immune to legal repercussions if they cross a certain line. Unauthorized access to systems, even with good intentions, can still be subject to legal – even criminal – action. Accessing

[1] The term «white hat hackers» and «black hat hackers» derived from old cheaply produced western movies, where the good guy wears a white and the bad guy a black hat.
[2] See factsheet for ethical hackers of the FDPIC (last visited on 31.10.2023).

a computer system by exploiting a vulnerability often provides access to the data it contains. In cases where personal data is involved, white hat hackers must also comply with the Federal Act on Data Protection (FADP). Accessing, downloading and disclosure of personal data constitute "processing" within the meaning of art. 5 lit. d FADP.

White hat hackers must, for example, comply with the principle of lawfulness (art. 6 para. 1 FADP) and the principle of good faith or proportionality (art. 6 para. 2 FADP). The principle of good faith requires that the white hat hacker does not have a hidden agenda or harms the system operator. The principle of proportionality requires that any processing of personal data should only occur when necessary to achieve the intended objective. This means that data should only be accessed if necessary and not kept any longer than needed.

> "
>
> WHILE WHITE HAT HACKERS OPERATE WITH NOBLE INTENTIONS, THEY ARE NOT IMMUNE TO LEGAL REPERCUSSIONS IF THEY CROSS A CERTAIN LINE.

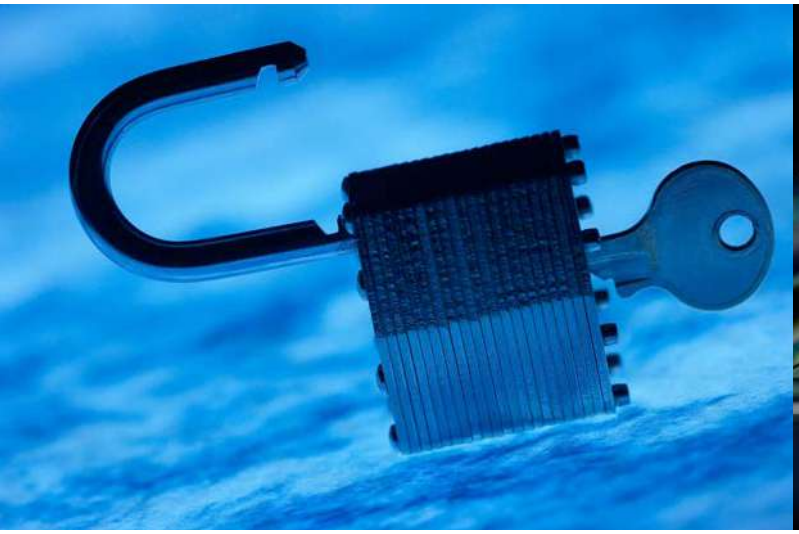
Legal risks for white hat hackers

White hat hackers' activities may lead to infringement of civil law, criminal law or administrative law. Risks under civil law can arise if a white hat hacker was not engaged by the controller of the personal data or the operator of the IT system, but rather acts on its own behalf. In such cases, it is possible that the system operator or the data subjects concerned file a civil claim. However, if white hat hackers act in good faith, limit their processing to a minimum and comply with the principles of personal data processing, the risk for civil claims can be minimized.

In addition to civil risk, white hat hackers are exposed to the risk of criminal prosecution according to the Swiss Criminal Code (SCC)[3]. Some of the behaviors such as the hackers' aim to enrich themselves are by definition incompatible with white hat hackers. Others, such as obtaining personal data without authorization can be committed even if the hacker behaves in an honest and noble manner. Those offences, however, are often only prosecuted on request by the injured party. If the hacker was engaged by an organization, the hacker does normally not risk any criminal prosecution.

Lastly, there are risks under administrative law according to art. 49 ff. FADP. If it appears that the white hat hacker did not comply with the FADP, the FDPIC can open an investigation and order administrative measures against the hacker. This aspect must be pointed out since the FDPIC cannot offer a guarantee of anonymity to the white hat hacker.

Thus, white hat hackers must operate within clear ethical guidelines and obtain proper authorization before conducting any security assessments. It is crucial that white hat hackers main-tain records of all activities. Thorough documentation serves as evidence of authorized access and helps establish the legitimacy of their actions.



[3] Relevant are articles 143 (unauthorized obtaining of data), 143bis (unauthorized access to a data processing system) and 179^{novies} (obtaining personal data without authorization) SCC.

What should organizations be aware of when engaging ethical hackers?

It is also important for organizations that engage white hat hackers to provide specific guidance and define the exact scope. The tasks for the ethical hackers depend on what exactly a company wants to achieve. The focus of interest is often cross-client data access[4] to systems, normal users with privileged admin rights, or even management portals that are more or less open to the internet. This usually involves access to email systems and HR applications, as salary and financial data are particularly sensitive.

Additionally, the proper selection of hackers is also important. Only professional hackers should be engaged. The price charged in proportion to the requested tasks can be an indication for professionalism (if a disproportionally low amount is charged, this should make one think twice whether to hire someone), also reviews and recommendations on blogs and other publications.

Lastly, it should not be underestimated that the results of white hat hackers are not exhaustive. Just because one hacker did not find any vulnerabilities does not mean that there are not any. Due to time and knowledge constraints and since technology evolves constantly, it is impossible for white hat hackers to find all weak points in the system.

To sum up, Swiss law provides a supportive framework for white hat hackers. By adhering to ethical guidelines and obtaining proper authorization, these professionals can play a crucial role in safeguarding the digital landscape.

Julia Bhend and Sena Hangartner
Probst Partner AG

> WHILE WHITE HAT HACKERS OPERATE WITH NOBLE INTENTIONS, THEY ARE NOT IMMUNE TO LEGAL REPERCUSSIONS IF THEY CROSS A CERTAIN LINE.
>
> Julia Bhend
> *Probst Partner AG*

[4] Cross-client data access means to gain access from one client to another client, which is possible since the data is not specific to any but belongs to all clients. The hacker can open the system client and change the coding. Such kind of attacks are very difficult to detect.

A dawn of a new era in India: India's First Ever Personal Data Protection Law

Previous Data Protection Law Regime in India

Earlier, there were no data protection legislations in India. The Information Technology Act, 2000 ("IT Act") and Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 ("SPDI Rules") were the only legislations for all data related things.

Digital Personal Data Protection Act, 2023

The Digital Personal Data Protection Act, 2023 received the assent of the President on the 11th August, 2023. The Act protects digital personal data by providing for the obligations of Data Fiduciaries (that is, persons, companies and government entities who process data) for data processing (that is, collection, storage or any other operation on personal data); the rights and duties of Data Principals (that is, the person to whom the data relates); and Financial penalties for breach of rights, duties and obligations. It seeks to introduce data protection law with minimum disruption while ensuring necessary change in the way Data Fiduciaries process data. It has introduced a unique Data Principal right – the right to nominate. Using this right, Data Principals can assign a representative to exercise their right in case of incapacity or death. By using the word "she" instead of "he", for the first time it acknowledges women in Parliamentary law-making. It safeguards the personal data of children also by mandating prior parental consent before processing of the personal data of children. It does not permit processing which is detrimental to well-being of children or involves their tracking, behavioral monitoring or targeted advertising.

Applicability

The Act applies (a) to the processing of digital personal data within the territory of India, where the personal data is collected - (i) in digital form; or (ii) in non-digital form and digitised subsequently; and (b) to processing of digital personal data outside the territory of India, if such processing is in connection with any activity related to offering of goods or services to Data Principals within the territory of India.

The Act shall not apply to (i) to personal data processed by an individual for any personal or domestic purpose; and (ii) personal data is made or caused to be made publicly available by - (A) the Data principal to whom such personal data relates; or (B) any other person who is under an obligation under any law for the time being in force in India to make such personal data publicly available.

Grounds for processing Personal Data

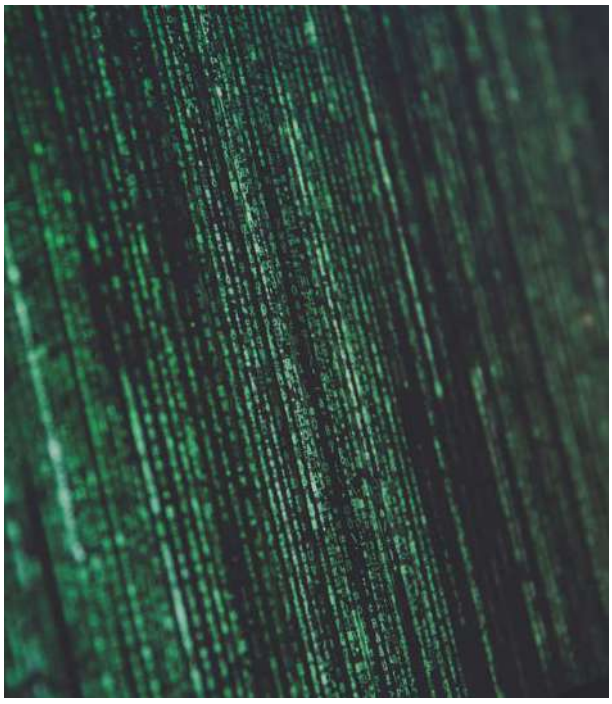
The grounds for processing Personal Data include a lawful purpose, purpose for which the Data Principal has given her consent; or for certain legitimate uses.

Notice, Consent & Withdrawal of Consent

The Act requires the Data Fiduciary to give a notice to the Data Principal while asking for her Consent to process her personal data. The consent given by the Data Principal shall be free, specific, informed, unconditional and unambiguous with a clear affirmative action, and shall signify an agreement to the processing of her personal data for the specified purpose and be limited to such personal data as is necessary for such specified purpose. Data Principal shall have the right to withdraw her consent at any time, with the ease of doing so being comparable to the ease with which such consent was given. The Data Principal may give, manage, review or withdraw her consent to the Data Fiduciary through a Consent Manager. The Consent Manager shall be accountable to the Data Principal and shall act on her behalf. Every Consent Manager shall be registered with the Board.

Rights of Data Principal

The Act provides for various rights of Data Principal which include Right to access information about personal data, Right to correction, completion, updation and erasure of personal data, Right of grievance redressal and Right to nominate.



Duties of Data Fiduciary

A data fiduciary shall protect personal data in its possession or under its control, including in respect of any processing undertaken by the data processor or on data fiduciary's behalf by a data processor, by taking reasonable security safeguards to prevent personal data breach as the Act does not directly impose any obligation on data processors.

The Act provides certain obligations of the Data Fiduciary which interalia include engaging with a Data Processor to process personal data on its behalf only under a valid contract, to implement technical and organizational measures to ensure effective observance with the Act, to establish an effective mechanism to redress the grievances of Data Principals, to delete and cause its Data Processor to erase data as soon as the purpose is accomplished and to report personal data breaches to Data Protection Board and Data Principals.

Significant Data Fiduciary (SDF) – Criteria to identify SDF

The Act provides criteria for Assessment of class of Data Fiduciaries as Significant Data Fiduciary which includes the volume and sensitivity of personal data processed, risk to the rights of data principal, potential impact on the sovereignty and integrity of India, risk to electoral democracy, security of the State and public order.

Additional obligations of SDF

In addition to the general obligations of a Data Fiduciary, a SDF is required to appoint a data protection officer based in India, appoint an independent auditor to carry out periodic data audits and conduct Data Protection Impact Assessment periodically.

Penalty

The Data Protection Board has the power to issue penalties up to INR 250 crore.

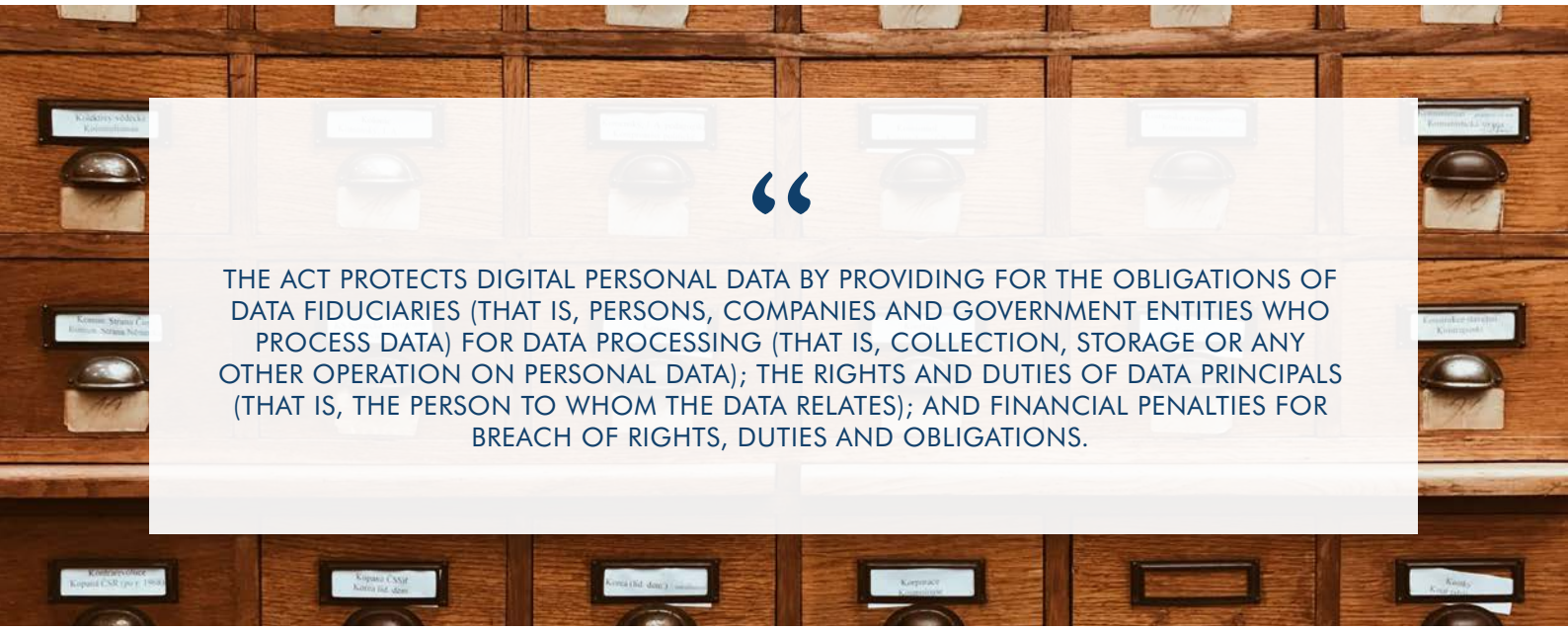
The Digital Personal Data Protection Board

The Act provides for establishment of a Board to be called the Data Protection Board of India. It shall consist of a chairperson and other members, to be appointed by the Central Government. The Board will function as an independent body and shall, as far as practicable, function as a digital office, with the receipt of complaints and the allocation, hearing and pronouncement of decisions in respect of the same being digital by design, and adopt such techno-legal measures as may be prescribed.

The DPDP Rules drafted, ready to be rolled out shortly

Although the DPDP Act has been enacted, it has not yet come into force. The Act is expected to be implemented in a phased manner. The DPDP Act provides significant rule-making powers to the central government relating to the implementation of data protection & privacy policies and other compliances by various stakeholders including Data Fiduciaries, Data Principal, Consent Manager etc. The government has drawn up the draft rules under the Digital Personal Data Protection (DPDP) Act and will be released soon. Parallelly, the digital architecture for the Data Protection Board will be developed. The DPDP Act requires the notification of 25 sets of rules to enable the enactment of the Act. All 25 sets will be released for public consultation in one go and will be notified at the same time.

Rahul Khosla
ILG



> “
>
> THE ACT PROTECTS DIGITAL PERSONAL DATA BY PROVIDING FOR THE OBLIGATIONS OF DATA FIDUCIARIES (THAT IS, PERSONS, COMPANIES AND GOVERNMENT ENTITIES WHO PROCESS DATA) FOR DATA PROCESSING (THAT IS, COLLECTION, STORAGE OR ANY OTHER OPERATION ON PERSONAL DATA); THE RIGHTS AND DUTIES OF DATA PRINCIPALS (THAT IS, THE PERSON TO WHOM THE DATA RELATES); AND FINANCIAL PENALTIES FOR BREACH OF RIGHTS, DUTIES AND OBLIGATIONS.

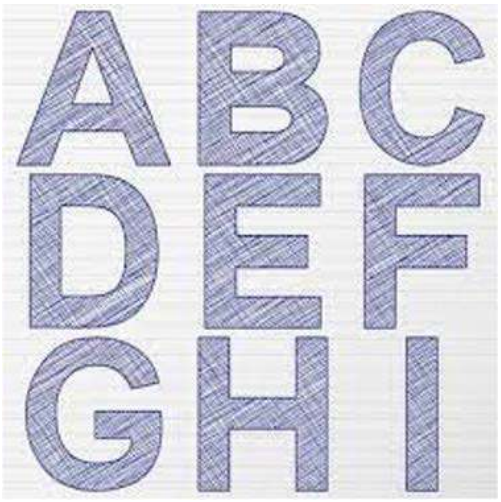
Eight questions to ask before you use AI in your organisation - and an answer to the question "is this OK?..."

If your team says to you about a particular AI tool (the one that they've been using but for which they now need your blessing) "this is OK isn't it...."
...You're going to need an answer that keeps you and your team on the right side of the law, but which is also helpful. An unqualified "it depends" probably won't do.

Fortunately, as far as the UK is concerned the ICO have partly answered that question – by highlighting eight questions that need to be answered for any AI project.

...But eight is a lot to remember – so how do you come up with an answer, on the spot that you can offer in response. In this article I have a suggestion which might help.
Here I have a confession. I love mnemonics – words that spell out something that would otherwise be difficult to remember. I relied on them throughout university and law school and have used them ever since. So – here's one that you might find useful when faced with the question (about AI) – "this is OK, isn't it...")

It follows the letters "A" to "I" alphabetically.



All are based on the questions suggested by the ICO in its recent guidance (which was itself a considerably condensed summary of the white paper toolkit and other resources on its site - so are by no means comprehensive)
But if you're using an AI solution that uses personal data then, as a starting point at least there are a few questions you can ask yourself (and your organisation) - by going through the letters "A" to "I"...

A is for "Automated Decision Making"

Will the AI be used to subject individuals to automated decisions (e.g job applications, eligibility for insurance)?
If so – and these have legal or similarly significant effects, then individuals have rights under Article 22 of UK GDPR to object to that automated decision making.

B is for "Basis" - What is your lawful basis for processing personal data?

If you are processing personal data you must identify an appropriate lawful basis, such as consent or legitimate interests.
On what basis are you processing data using AI? Do you have consent? Is this pursuant to a contract, do you have a legitimate interest or another legal basis?

C is for "Controller" – Are you Controller or processor?

If you are developing generative AI using personal data, you have obligations as the data controller.
If you are using or adapting models developed by others, you may be a controller, joint controller, independent controller or a processor.
You need to work out what your relationship is with the data subject in order to work out your obligations and make sure you have the right contractual basis for that.

D is for "Data Protection Impact Assessment" (DPIA)?

You must assess and mitigate any data protection risks using a DPIA before you start processing personal data.
Your DPIA will need to be kept up to date as things change.

E is for "Explicit" – have you told data subjects?
You must be explicit about the processing, making information about the processing publicly accessible unless an exemption applies.
Unless it takes disproportionate effort, you must communicate this information directly to the individuals the data relates to.

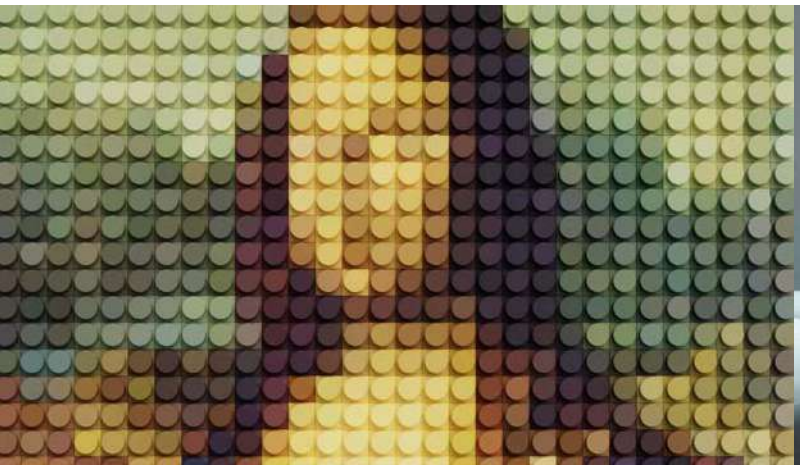
F is for "Fulfil" – does your use of data fulfil the purpose you stated?
You must collect only the data that is adequate to fulfil your stated purpose. The data should be relevant and limited to what is necessary.

G and H are for "Guard" against "Harmful" security risks?
This is about data security. Consider the various risks of cyber attack and the use of (for instance) Chat GPT plugins. *(You might think I cheated with the G & H referring to the same question, but it's my mnemonic – so I'm sticking with it!)*

I is for "Individual rights"
You must be able to respond to people's requests for access, rectification or other individual rights. How will you respond to DSARs that involve the AI system that you are using?

Once you have the answers to these questions you're in a considerably better position in terms of your AI govenance (at least from a UK data perspective).

Richard Nicholas
Browne Jacobson



ITALY •

Personal data processing for marketing and profiling purposes: the Italian data protection authority sanctions Benetton.

In the decision dated 27 April 2023 issued against Benetton, a historic Italian textile company, the Italian Data Protection Authority addresses critical profiles in the area of security measures for the processing of personal data for marketing and profiling purposes.

Benetton was fined EUR 240,000 for unlawfully processing of personal data of a significant number of customers and former customers, and in particular for failing to adopt adequate security measures and storing personal data for marketing and profiling purposes without time limits.

The investigation against Benetton had been initiated ex officio in 2019, based on the inspections planned by the Data Protection Authority, first remotely and then at the company's headquarters, with a technical assessment of the company's databases related to processing for marketing and profiling purposes. The investigative activity had in particular concerned the information banner regarding the use of cookies of one of the websites owned by the company and the processing of data of customers members of the Benetton loyalty program.

The investigation carried out by the Authority highlighted the failure to adopt adequate security measures with reference to the processing of personal data of the members of the loyalty program - and therefore data related to purchasing preferences of a relevant number of customers and former customers.

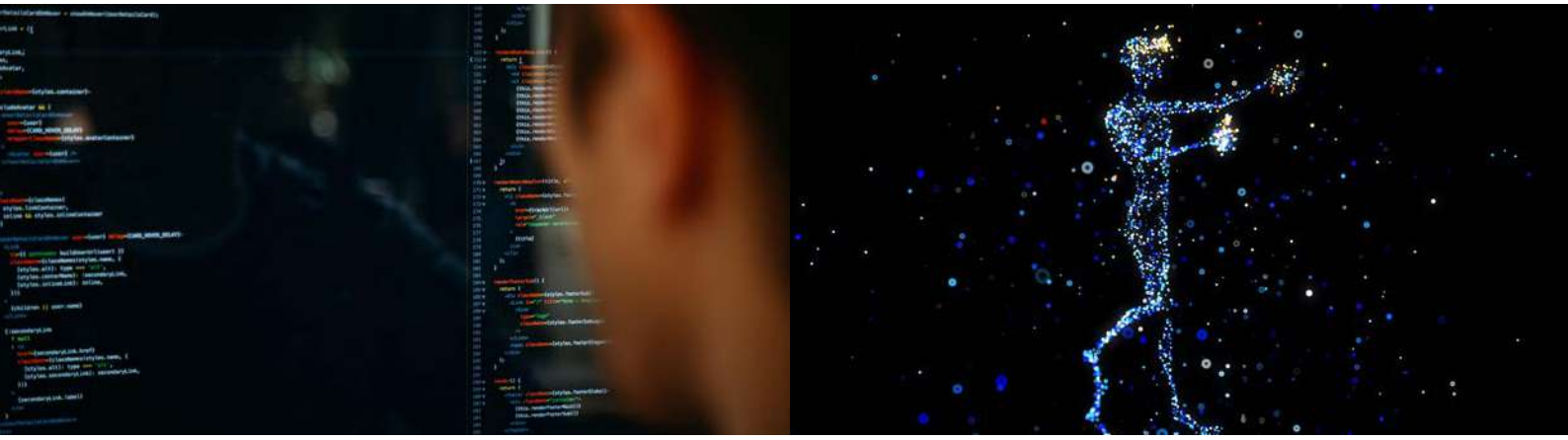
The Data Protection Authority in particular pointed out a violation of Article 32, paragraph 1, letter b) and d) GDPR with reference to the fact that: the PC used in the stores for data collection did not provide for limitations in terms of operation (allowing, for example, screenshots); customers data were accessible by all store employees in 7 European countries; again, the data were accessible from any device connected to the Internet with a single password and account, making it, among other things, impossible to identify the responsible party in case of a data breach.

The Italian Authority also confirmed a violation of Article 32, paragraph 1, letter d) GDPR because a procedure to regularly verify the effectiveness of the technical and organizational measures necessary to ensure data security was absent.

The company was also condemned for violation of the principles of minimization and limitation of storage (Article 5, paragraph 1, letter c) for retaining a significant amount of data of individuals subscribed to the newsletter after the service was deactivated.

Again, with reference to the data retention period, the Authority points out that the retention of personal data for marketing and profiling purposes for a period of ten years is clearly excessive and recalls in this regard a long-standing ruling of the same Authority on loyalty programs and consumer guarantees. In such ruling dated 2005, and thus well before the GDPR came into force, the Authority had identified 12 months as the data retention period for profiling purposes and 24 months as the retention period for marketing purposes. Under the GDPR, the retention period must be identified by the data controller, who must be able to justify and document such decision, but the periods pointed out by the Italian Data Protection Authority for processing for marketing and profiling purposes in such ruling remain an important benchmark in Italy. The Authority has therefore ordered Benetton to adopt organizational and technical solutions that ensure that data retention complies with the provisions of the regulation.

Marta Margiocco
Cocuzza & Associati Studio Legale



CZECH REPUBLIC •

For EU-U.S. data transfers, is Data Privacy Framework the light at the end of the tunnel?

Ever since the European Courf of Justice (CJEU) released its decision no. C-311/18 (Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems), also known as Schrems II, which shut down the Privacy Shield framework, due to it not providing adequate protection of the data subjects, the EU-U.S. data transmission was in a great need of something that would unite the requirements again and stop the legal uncertainty that ensued after it.

Before the Data Privacy Framework (DPF) came into force, companies still were able to use the Privacy Shield certification, but only as a supplement to other measures. Therefore, everyone had to rely on standard contractual clauses between data controllers and data processors, which were officially accepted in the Commission decision no. 2010/87/EU.

Finally, on 10 July 2023 the Commission implementing decision came into force which aimed to set up the DPF which was followed by the Department of Commerce´s International Trade Administration´s operational update on the implementation of the EU-U.S. DPF. The Privacy Shield certificates were automatically converted to DPF while companies were obliged to achieve compliance with the EU-U.S DPF principles by 10 October 2023.

By implementing this new system, the EU says that all the companies registered under the DPF in the U.S. are safe and can be provided with protected data. This mainly aims to end the uncertainty of standard contractual clauses and the fear of violating data protection law that ensued after the Schrems II decision.

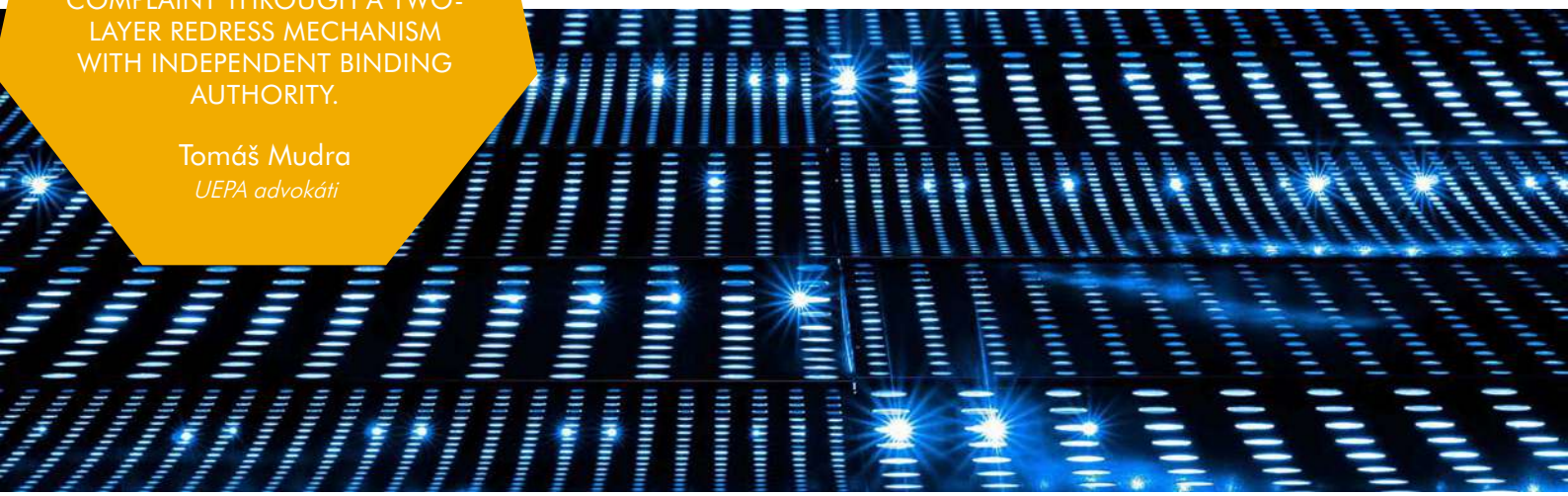
DPF brings one major change and that is the new redress mechanism. Individuals can now file a complaint through a two-layer redress mechanism with independent binding authority. Individuals do not have to demonstrate, that their data was in fact collected by U.S. intelligence agencies. The complaints are to be filed to their national protection authority, which will ensure that the complaint will be properly transmitted and inform the individual about the procedure. The European Data Protection Board will then transmit the complaints to the U.S. and there the complaints are to be investigated by the Civil Liberties Protection Officer and individuals will have the possibility to appeal their decision before the newly created Data Protection Review Court, which is composed, of members from outside the U.S. government. The court then has powers to investigate complaints from EU individuals, including obtaining relevant information from intelligence agencies, and can take binding remedial decisions. In each case, the Court is to select a special advocate with relevant experience to represent the complainant´s interests and to inform the Court of factual and legal aspects of the case.

The European Center for Digital rights (NOYB), which is responsible for the Privacy Shield and Safe Harbor shutdown, has however declared its intent to challenge the DPF. The NOYB calls the new framework a copycat of the two previous attempts to make data transfers with U.S. safe. The major problem regarding the U.S.-EU data transfers is however the U.S. surveillance law under FISA 702, which authorizes public authorities to have access to any and all personal data if acting in the interest of national security or investigating a crime. The NOYB says that the challenge to CJEU is ready to be filed and is just waiting for the new system to set in.

It should be noted that the main reason for the Privacy Shield shutdown was there not being any authority in the U.S. to enforce the data protection against public authorities such as the NSA or FBI. The CJEU said that the Ombudsman established by the Privacy Shield was not enough. In contrast, the DPF comes with a new redress mechanism with an impartial court and therefore, in our opinion, it might be able to stand up to the upcoming challenge and if so, it also could be able to put an end to the uncertainty that came after the shut-down and companies being forced to use standard contractual clauses.

Tomáš Mudra
UEPA advokáti

> DPF BRINGS ONE MAJOR CHANGE AND THAT IS THE NEW REDRESS MECHANISM. INDIVIDUALS CAN NOW FILE A COMPLAINT THROUGH A TWO-LAYER REDRESS MECHANISM WITH INDEPENDENT BINDING AUTHORITY.
>
> Tomáš Mudra
> *UEPA advokáti*

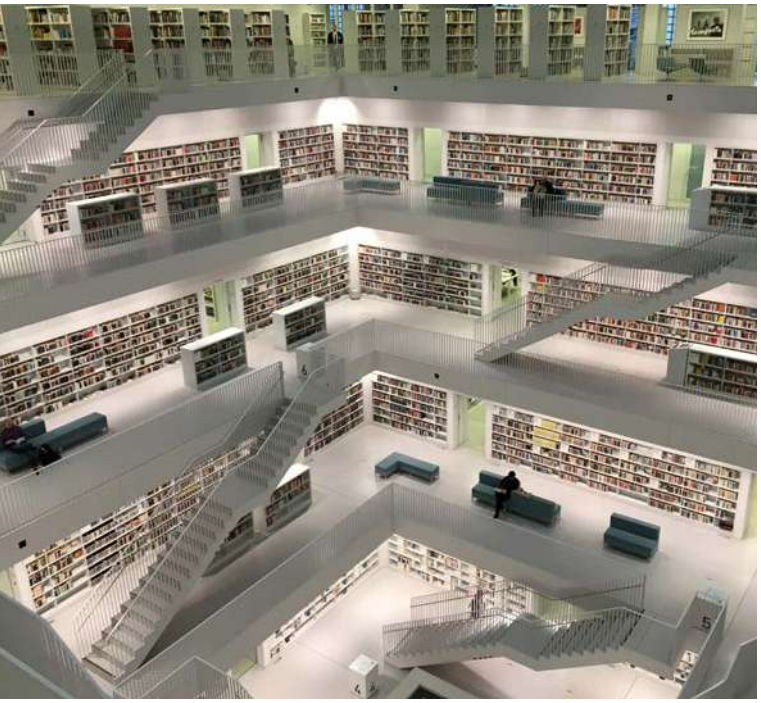


GERMANY •

Compensation for data protection incidents in Germany

"German courts are rather reluctant to award non-material damages for data protection violations; however, there are already a relatively large number of individual decisions in this regard."

One pillar for strengthening data protection in Europe was, in particular, the clarification that data subjects should also be better able to assert their own claims. To this end, it was clarified in Art. 82 GDPR, among other things, that data subjects are entitled to compensation for any damage they have suffered as a result of a data protection breach. It is clear from the wording of the regulation that it is not only about compensation for material damage, but that non-material damage can also be compensated.



In Germany, there have so far only been very few cases in which the courts have exceptionally awarded compensation for non-material damage to injured parties. So far, only small amounts have been awarded as compensation for pain and suffering. The best-known cases relate to payments for injuries sustained in traffic accidents. Otherwise, non-material damages have only been awarded to a very limited extent in some cases of violation of personal rights, for example in the case of unlawful media coverage of celebrities. So far, the courts have always argued that only true damages should be compensated, but that the injured party should not be enriched by such an incident. It is also feared that compensation for non-material damage will quickly lead to the responsible party being punished. The supervisory authorities, however, are responsible for punishing violations in this area and can also impose fines.

As Germany has no experience with immaterial damages in this respect, the courts in Germany first wanted to wait for the European Court of Justice to clarify some fundamental issues. A decision by the ECJ, which is based on proceedings from Austria, has provided more clarity in this respect (ECJ, judgment of 4.5.2023 - case no. C-300/21). In its decision, the ECJ found that the terms "material and non-material damage" and «compensation» are autonomous concepts of EU law and must therefore be interpreted uniformly in all Member States. It is also clear from the wording of the provision in Art. 82 GDPR that not every breach of the GDPR is sufficient for a claim for damages. The cumulative requirements for such a claim are a breach of the GDPR, specific material or non-material damage and, finally, a causal link between the damage and the breach. This is also supported by the recitals, according to which the occurrence of damage is not the necessary consequence of a breach of the GDPR. However, the court found that the right to compensation for non-material damage does not depend on the materiality of the damage. A broad understanding of the term «damage» applies. The definition of a materiality threshold is incompatible with this. The possibly different assessment of this materiality by the courts would also be contrary to a uniform interpretation. However, the decision also emphasized that the lack of a materiality requirement does not exempt the person entitled to claim from having to prove concrete non-material damage caused by a GDPR violation.

This decision is significant in that concrete damage was confirmed as a necessary prerequisite for a claim under Art. 28 GDPR. It is clear from the ECJ's explanations that damage must always be demonstrated and must not be presumed. In the past, for example, some German labor courts have assumed non-material damage in the event of a breach of the one-month period for processing a claim for information in accordance with Art. 15 para. 1, 3 GDPR without this being proven (e.g. ArbG Bamberg, judgment of 11.5.2022 - Ref. 2 Ca 942/20; ArbG Oldenburg, judgment of. 9.2.2023 - Ref. 3 Ca 150/21). This will no longer be possible in this form. Compensation for non-material damages is also not limited to damages that have reached a certain degree of materiality.

However, this means that non-material damages have not yet been conclusively clarified from a German perspective. In a ruling dated September 26, 2023, the Federal Court of Justice (BGH) referred questions to the ECJ regarding, among other things, the concept of non-material damage within the meaning of Art. 82 GDPR (BGH, judgment of 26.9.2023 - Ref. VI ZR 97/22). In the initial dispute, the plaintiff claimed that he had suffered damage due to the fact that a message intended only for the plaintiff was also sent to a

third party during the application process at the defendant. Among other things, the message stated that the defendant could not meet the plaintiff's salary expectations. The plaintiff feared that this sensitive data could be passed on or that an advantage could be gained as a result; he himself would not have passed the data on to third parties. The BGH's questions in this regard relate, among other things, to whether mere negative feelings such as anger, displeasure, concern or fear are sufficient for the assumption of material damage within the meaning of Art. 82 GDPR. Furthermore, the BGH would like to know whether the degree of fault of the controller is a relevant aspect when assessing the amount of damages and whether a claim for injunctive relief to which the data subject is entitled should be taken into account. It remains to be seen how the ECJ will position itself on the BGH's questions.

The questions that the BGH has now referred to the ECJ show that the German courts remain reluctant to grant larger amounts of compensation for non-material damage in the event of data protection breaches. The labor courts were still relatively generous when it came to the processing of employee data. Civil courts have continued to reject claims for damages in many cases following the ECJ's first ruling. Most recently, for example, the Higher Regional Court of Hamm refused to award damages to Facebook users after account data was leaked from Facebook and misused by third parties (Higher Regional Court of Hamm, judgment of 15.08.2023, ref. 7 U 19/23). A Facebook user therefore asserted a claim for damages in the amount of EUR 1,000 because the disclosure of his data would have resulted in a loss of control. The court assumed a breach of data protection and confirmed that there is no materiality threshold for damages. Nevertheless, the court did not want to recognize any compensable damage in these and other cases. It remains to be seen whether the German courts will change their restrictive position if other countries deal more generously with claims for damages. So far, there are no signs of such a development.

Dr. Sebastian Meyer
BRANDI Rechtsanwälte

DATA, INFORMATION & CYBER LAW

Members & Contacts

Laurent Badiane
klein • wenner
19 rue Danielle Casanova, 75001 Paris, France
T: +33 1 44 95 20 00
E: laurent.badiane@kleinwenner.eu

Michiel Beutels
Litiguard Law Firm
Tabakvest 52-54, 2000 Antwerpen
T: +32 (0)3 205 68 40
E: mb@litiguard.eu

Julia Bhend
Probst Partner AG
Bahnhofplatz 18, CH-8401 Winterthur, Switzerland
T: +41 52 269 14 00
E: julia.bhend@probstpartner.ch

Matthieu Bourgeois
klein • wenner
19 rue Danielle Casanova, 75001 Paris, France
T: +33 1 44 95 20 00
E: matthieu.bourgeois@kleinwenner.eu

Theresa Castelan
klein • wenner
19 rue Danielle Casanova, 75001 Paris, France
T: +33 1 44 95 20 00
E: theresa.castelan@kleinwenner.eu

Jeanne Kelly
Browne Jacobson
6-7 Fitzwilliam Square East Dublin 2D02 Y447 Ireland
T: +35315743915
E: jeanne.kelly@brownejacobson.com

Rahul Khosla
ILG
F-42, East of Kailash, New Delhi 110065, India
T: +91 11 4657 5667
E: rahul@ilgindia.com

Marta Margiocco
Cocuzza & Associati Studio Legale
Via San Giovanni Sul Muro 18, 20121 Milano, Italy
T: +39 02-866096
E: mmargiocco@cocuzzaeassociati.it

Julia Mascini
Valegis Advocaten
Apollolaan 151, 1077 AR Amsterdam, The Netherlands
T: +31 (0)6 82 13 53 62
E: j.mascini@valegis.com

Michał Matuszczak
Babiaczyk, Skrocki i Wspólnicy Sp. K
ul. Wyspianskiego 43, 60 – 751 Poznan, Poland
T: +48 61 8441 733
E: m.matuszczak@bsiw.pl

Sebastian Meyer
BRANDI Rechtsanwälte
Adenauerplatz 1, 33602 Bielefeld, Germany
T: +49 521 96535 812
E: sebastian.meyer(at)brandi.net

Razvan Miutescu
Whiteford
7 St. Paul Street, Baltimore, MD 21202-1636, USA
T: +1 410 347 8744
E: rmiutescu@whitefordlaw.com

S. Keith Moulsdale
Whiteford
7 St. Paul Street, Baltimore, MD 21202-1636, USA
T: +1 410 347 8721
E: skmoulsdale@whitefordlaw.com

Tomáš Mudra
UEPA advokáti s.r.o.
Voctárova 2449/5, 180 00 Prague, Czech Republic
T: +420 234 707 444
E: TMU@uepa.cz

Richard Nicholas
Browne Jacobson
103 Colmore Row, Birmingham B3 3AG, The UK
T: +44 1 21 237 3992
E: richard.nicholas@brownejacobson.com

READ OUR ANNUAL REPORT 2022/2023

CONNECT WITH US

PANGEANET
INTERNATIONAL NETWORK OF INDEPENDENT LAW FIRMS

To find our other publications and newsletters

CLICK HERE

Email: info@pangea-net.org
Website: www.pangea-net.org
Linkedin: /company/pangeanet