Privacy Flash – Issue 21

Privacy at your fingertips

Privacy is becoming increasingly important to everyday business. Legal developments and regulators' increasing attention to privacy are two of the key drivers behind this.

The aim of the Privacy Flash is to provide monthly updates on global regulatory developments, as well as relevant news and information on upcoming events in the field of data protection and privacy.

Previous issues are available on our website, via the 2015 | 2016 | 2017 | 2018 archive.

For additional information, to subscribe, or to suggest improvements to the Privacy Flash, please email BEPrivacyFlash@deloitte.com.

To unsubscribe, please send us an email using this link.

Highlights

- European Commission confirms post-Brexit UK as a third country
- WP 29 draft guidelines on several major compliance topics, such as consent and transparency
- Privacy Shield survives first annual joint review
- CNIL publishes guidance for processors

News

DG JUST: Brexit qualifies UK as third country for international data transfers

On 9 January 2018, the European Commission (DG Just) issued a notice to stakeholders on the Withdrawal of the United Kingdom from the European Union and its implications on data protection rules. This notice establishes the status of the UK as a third country, following its decision to leave the EU.

As a result, all future transfers of personal data to the UK will be subject to the obligations and rules of the GDPR on transfer of personal data to third countries. Therefore, a transfer of personal data to the UK will only be possible if the controller or processor puts in place appropriate safeguards. An adequate level of data protection can be provided by standard data protection clauses, binding corporate rules, approved codes of conduct or approved certification mechanisms or derogations.

With this notice, the European Commission stresses that "preparing for the withdrawal is not just a matter for EU and national authorities but also for private parties". Hence, organisations and businesses must quickly take the necessary steps to identify any UK-oriented data transfers and put in place the necessary safeguards.

WP 29 draft guidelines on automated decision-making and profiling

On 17 October 2017, the Article 29 Working Party ("WP 29") published its draft guidelines on profiling and automated individual decision-making ("guidelines") in an attempt to clarify uncertainties in relation to these processing activities under the General Data Protection Regulation ("GDPR"). The WP 29 recognizes the benefits that profiling and automated decision-making can bring for individuals and organisations, as well as for the economy and society as a whole. However, these processing activities can also pose significant risks for an individual's rights and freedoms, which require the use of appropriate safeguards when carrying out profiling or automated individual decision-making activities.

The guidelines consist of five major sections. First, the WP 29 provides an overview of all definitions related to profiling and automated decision-making. It also reflects the GDPR's approach to these concepts. Here, the Working Party makes an interesting distinction between three potential ways in which profiling may be used: general profiling, decision-making based on profiling and solely automated decision-making, including profiling.

In a second section, the WP 29 further explains the provisions of Article 22 GDPR. According to the Working Party, Article 22 states that, as a rule, there is a prohibition on fully automated individual decision-making, including profiling that has a legal or similarly significant effect. As with every rule, there are some exceptions. In case one of the exceptions applies, measures should be in place to safeguard the data subject's rights and freedoms and legitimate interests. The WP 29 also provides clarifications in this section on the meaning of 'based solely on automated processing' and 'legal or similarly significant effects'. In addition, guidance is being provided on the appropriate safeguards controllers have to implement in case they rely on one of the exceptions to the general prohibition.

The Working Party points out the right to be informed, the right of access and the right not to be subject to a decision based solely on automated decision-making, are examples of such specific safeguards.

An interesting discussion has arisen as to the approach taken by the WP 29 in this guidance. As mentioned, according to the Working Party, the GDPR contains a prohibition on solely automated decision-making that includes profiling, with limited exceptions involving explicit consent or performance of contract. This statement has triggered some controversy as to the meaning and the value of the provisions in Article 22. Some are convinced that the provision should be interpreted as a right of the data subject rather than a prohibition for data controllers to carry out these processing activities in the first place. According to them, this interpretation could have far-reaching consequences if not corrected. Whether the WP 29 will change its position on this matter remains to be seen.

Next, the WP 29 discusses the general provisions of the GDPR (such as data protection principles, lawful grounds for processing, special categories of personal data, rights of the data subject) in relation to profiling and automated individual decision-making.

The fourth section of the guidelines covers profiling in relation to children. According to the WP 29, there is no absolute prohibition of applying solely automated individual decision-making, including profiling, to children. However, the Working Party recommends that, where possible, controllers should not rely on the exceptions in Article 22(2) GDPR to justify these processing activities in relation to children. Since there is a need for particular protection for children, as reflected in recital 38 of the GDPR, the WP 29 states that organizations should, in general, refrain from profiling children for marketing purposes.

The WP 29 describes the cases in which a DPIA should be carried out. Importantly, it indicates that both not wholly as well as solely automated decision-making, including profiling, may trigger the need to carry out a DPIA. Lastly, the guidelines also articulate a list of good practice recommendations to assist controllers in meeting the GDPR requirements in relation to profiling and automated decision-making. These include direction with regards to providing information using layered notices, but also examples of additional safeguards when profiling, such as algorithmic auditing and anonymization or pseudonymization techniques.

WP 29 draft guidelines on consent

On 28 November 2017, the Article 29 Working Party ("WP 29") released its draft guidelines on consent which provide a thorough analysis of the notion. The guidelines build upon the previous opinion of the WP 29 on consent, dating back to 2011 and focus on the changes created by the GDPR as compared to the Data Protection Directive (Directive 95/46/EC) and the e-Privacy Directive. The clarifications made by WP 29 will also be relevant for the interpretation of this notion in the draft e-Privacy Regulation, since consent used in this upcoming Regulation remains linked to the notion of consent in the GDPR. As for the existing e-Privacy Directive, references to Directive 95/46/EC shall be interpreted as references to the GDPR. In essence, this means that the GDPR conditions for obtaining valid consent are applicable both in relation to the e-Privacy Directive and the future e-Privacy Regulation.

In the guidelines, the WP 29 provides clarifications on the notion of consent, described in the GDPR as "*any **freely given**, **specific**, **informed** and **unambiguous***

indication of the data subject's wishes by which he or she, by a statement of by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her".

"Freely given" consent means that the data subject should have ab actual choice and control when consenting to the processing of his or her personal data. According to the Working Party, the biggest bottlenecks to comply with this requirement are the possibility of an imbalance of power between the controller and the data subject and the presence of conditionality. In case there is an imbalance of power, for example in relation to public authorities or in the employer-employee context, a data subject will have no realistic alternative than to accept the processing activities of the controller. In these situations, the use of consent is not entirely excluded, as there may be exceptional occasions where the data subject would not be compelled to consent out of fear for negative consequences.

The other bottleneck, described as conditionality, refers to "bundling" or "tying" of consent. Where consent for processing personal data is bundled to the acceptance of terms and conditions or tied to the provision of a contract or service and the processing of the personal data is not necessary for the performance of that contract, it will not be considered as freely given. As a counterpart of the fact that consent should be freely given, the controller should be able to demonstrate that consent can also be withdrawn without detriment, meaning without additional costs, deception, intimidation, coercion or significant negative consequences. If the controller is able to show that this is possible, this may assist in showing that consent was freely given in the first place.

Consent must also be "specific". The controller must apply the principle of purpose specification to avoid widening and blurring of the purposes for which personal data is processed (also known as "function creep"). To this extent, consent requests must be granular, and must keep information related to the consent separate from information on other matters (such as commercial terms and conditions). In principle, consent may cover different processing operations as long as they serve the same purpose.

Consent must be "informed". The WP 29 sums up the minimum content requirements that must be provided to a data subject and provides an overview of how this information should be provided by the controller. In general, the information should be easily understandable for the average person, clear and distinguishable from other matters and provided in an intelligible and easily accessible form. The controller should always keep in mind the kind of audience that provides personal data to the organization and should adapt the information provided taking this into account. A clear distinction is made between consent requested as part of a paper contract and via electronic means. Further specific guidance is provided in the WP 29 guidelines on transparency.

Lastly, consent should also be "unambiguous", meaning that a deliberate action to consent is needed from the data subject. This can be collected through a written or (recorded) oral statement, including by electronic means. In particular with respect to consent provided via electronic means, it may be necessary that a consent request interrupts the user experience to some extent to make the request effective, not making the request unnecessarily disruptive to the use of the service for which consent is being provided. In the electronic context, the WP 29 warns for "click fatigue", meaning that when consent is being asked too many times in an online environment, the actual warning effect of the consent mechanism diminishes. According to the Working Party, a way to prevent this is to

obtain consent from internet users via their browser settings, preferably in a granular way.

In some cases, the GDPR requires data controllers to obtain "explicit" consent from the data subject. The WP 29 provides an overview of the ways in which the explicit consent of a data subject can be collected, for example via an express written statement. According to the Working Party, an oral statement can also be sufficient.

The GDPR introduces additional obligations for controllers to obtain, maintain and demonstrate valid consent. Controllers can choose to demonstrate that these obligations have been fulfiled in a way that corresponds best to their daily operations. Regarding the withdrawal of consent, the GDPR codifies the existing interpretation of WP 29, stating that the controller must ensure that consent can be withdrawn as easy as it was given by the data subject and at any given time. This condition is part of a valid consent mechanism under the GDPR.

The guidelines also elaborate on obtaining consent from minors. Personal data processing shall only be lawful where the child is at least 16 years old, with a possibility for Member States to deviate and apply a lower age for digital consent that can not be lower than 13 years.

In order to obtain "informed" consent of a child, the controller must provide the information concerning the processing in a language that is understandable to a child. To assess whether the child in question has reached the appropriate age to consent (which may differ according to the applicable national law), WP 29 states that the controller is expected to make reasonable efforts to verify this. If the users state that they are over the age of digital consent, the controller should carry out appropriate checks to verify that this statement is true. The verification obligation of the controller should not lead to excessive data processing.

According to WP 29, consent obtained under Directive 95/46/EC remains valid in so far as it is in line with the conditions laid down in the GDPR. Since the GDPR raises the bar for consent to be valid, controllers are in many cases obliged to alter their consent mechanisms. As a consequence, all presumed consents (like pre-ticked boxes) will have to be renewed. On the other hand, the extended information obligations under the GDPR do not automatically render consent obtained before the GDPR was pronounced invalid. In any case, consent will have to be renewed in case it does not meet the GDPR standard. However, the guidelines do not (yet) elaborate on how this renewal should be carried out by the data controller.

WP 29 draft guidelines on transparency

On 12 December 2017, the Article 29 Working Party ('WP 29') published draft guidelines on the interpretation of the transparency principle under the GDPR. With these new guidelines, the Working Party aims at providing practical guidance and interpretative assistance concerning the GDPR transparency obligation.

Transparency, intrinsically linked to fairness and accountability, is one of the key building blocks of the new Regulation. In general, the principle entails the obligation for a data controller to inform data subjects properly. In practice, this translates into several information requirements that are to be respected throughout the lifecycle of data processing.

The guidelines consist of nine separate sections helping data controllers with the interpretation and practical implementation of transparency related concepts. One of the main issues addressed is 'information fatigue'. Today, data subjects are too often flooded with privacy-related information. This 'information overkill' is a source of many irritations in modern life society. Therefore, the Working Party states that it is up to the data controller to ensure that information is presented and communicated towards data subjects in an efficient and succinct manner. To fulfil this obligation, WP 29 addresses several options.

A first option consists of using layered privacy notices. The sheer volume of information that has to be provided stands in natural tension with the ability of individuals to easily process that information. Layered notices solve this issue as they allow data subjects to navigate directly towards the topic of their interest. The idea is to include in the first layer a clear overview of all available information on the processing of personal data. The secondary layers should then enable data subjects to access more detailed information regarding a specific topic.

A second option includes the use of 'push' and 'pull' notices. Push notices involve the provision of 'just-in-time' transparency information. According to the Working Party, 'just-in-time' is to be explained as the provision of specific privacy information in an ad hoc manner, as and when it is most relevant for the data subject to read. This allows splitting the information up – both in time and size – into more 'digestible' chunks. 'Pull notices' facilitate access to information by methods such as 'transparency dashboards', learn-more tutorials and permission management. The aforementioned 'transparency dashboard' consists of a single reference point from which data subjects can access privacy related information and manage their privacy settings and preferences. Via the dashboard they can either allow or prevent their data from being used for certain purposes. This is particularly useful when a service is being provided via various devices or apps. In the context of apps, the Working Party further states that privacy information should never be more than 'two clicks away'.

The guidelines further zoom in on several aspects and elements of transparency such as the use of basic privacy icons. In the Working Party's view, the effectiveness of such icons strongly depends on their standardization. In the end, the Working Party provides for a schedule, which summarizes the categories of information that must be provided under articles 13 and 14 GDPR.

Data controllers should be aware that transparency goes beyond the provision of appropriate privacy notices. The Working Party stresses on several occasions that transparency must be ensured in any relation or communication with data subjects (e.g. when data subjects exercise their privacy rights, in case of a data breach, etc.). Data controllers are advised to revisit all privacy notices and standard communications currently in place in order to ensure their compliance with GDPR information and transparency principles.

WP 29 guidance on sanctions

The Article 29 Working Party also published guidelines on the application and setting of administrative fines under the GDPR as laid out in Article 83.

In general, supervisory authorities must assess the facts of every case in order to impose a sanction that correctly responds to the nature, gravity and consequences of the breach. According to Article 83 (1), the corrective measure should be

effective, proportionate and dissuasive, taking into account the objective that the supervisory authority wishes to pursue.

Article 83 (2) further provides the criteria that supervisory authorities are expected to use when assessing if a fine should be imposed, and what its size should be. The Regulation further identifies two categories of infringements eliciting different maximum fines. Using non-compliant data processing agreements or failing to properly notify a data breach can give rise to a fine up to 10 million euros, or 2% of the global annual turnover. Violating consent requirements or not supporting international data transfers with an appropriate transfer mechanism, on the other hand, may be subject to a fine of maximum 20 million euros or 4% of the global annual turnover, whichever is the highest.

The Working Party explicitly stipulates that the concept of an undertaking refers to an economic unit, which may be formed by the parent company and all involved subsidiaries. This means that when a subsidiary is responsible for violating the GDPR, the annual turnover of the entire company will be considered for determining the amount of the fine.

One of the main purposes of the GDPR is to stimulate a consistent, high and equivalent level of protection in all the member states. While Article 58 grants supervisory authorities some flexibility in determining what corrective measure to use or fines to impose, a consistent approach for similar cases is expected. The Working Party also advises supervisory authorities to proactively exchange information regarding the practical application of their fining powers in order to achieve greater consistency amongst the different member states.

Supervisory authorities must always consider the nature, gravity and duration of the infringement. For minor infringements, corrective measures may include reprimands. A reprimand can also be more appropriate where a fine would constitute a disproportionate burden to a natural person. When determining the size of the fine, the supervisory authorities should take into account the following factors:

- The number of data subjects involved: in order to identify whether the breach is an isolated event or part of a more systemic breach;
- The scope and purpose of the processing concerned: the authorities should look into the how the organization has addressed the purpose limitation principle, purpose specification and compatible use;
- The level of damage suffered by the data subjects involved, taking into account the risk to their rights and freedoms;
- The duration of the infringement: the duration of the infringement may reveal willful conduct, failure to take appropriate preventive measures or an inability to put in place the required technical and organizational measures.

The intentional or negligent character of the infringement also plays a decisive role. Intentional breaches are obviously considered more severe than unintentional breaches. Hence, they are more likely to result in an administrative fine. Examples include unlawful processing authorized explicitly by the controller's executive management. It is the responsibility of any enterprise to adopt sufficient structures and policies to avoid such circumstances. Hence, any positive actions taken by an enterprise to that effect are also taken into account when determining the size of the fine.

The Working Party does not provide any detailed calculations regarding the size of the fines. Such insights will likely be provided through future enforcement action.

WP 29 draft guidelines on data breach notification

The GDPR includes the obligation to notify personal data breaches to the supervisory authority and to communicate the incident to individuals. In support of this high-impact innovation, the Article 29 Working Party has released draft guidelines on this matter.

In case of a data breach, the controller must notify the supervisory authority without undue delay and, where feasible, not later than 72 hours after having become aware of the breach. The Working Party explains that 'becoming aware' means 'having a reasonable degree of certainty that a security incident has occurred that has led to personal data being compromised'. The controller is not considered 'aware' during the first initial investigation of the incident, which should begin as soon as possible. Once the controller has identified the incident as having compromised personal data, it is considered to be 'aware' and must notify the supervisory authority if the breach represents a likely risk to individuals.
Processors must notify the controller without undue delay, meaning immediately.
Notifications of a data breach to a supervisory authority must contain at least the following information:

- The nature of the personal data breach: a description of the types of individuals whose data was affected by the breach, a description of the types of personal data that were affected and the number of personal data records affected;
- Name and contact details of the data protection officers or another point of contact;
- The likely consequences of the personal data breach and the measures taken or proposed measures to be taken by the controller in order to address the personal data breach.

If this information cannot be provided within 72 hours, a delayed or phased notification is (exceptionally) permissible. In those cases, the reason for the delayed notification has to be spelled out. When faced with complex breaches requiring significant forensic effort, organizations can also notify the authority using a phased approach and provide more information as soon as available.

Breaches which are unlikely to result in a risk to the rights and freedoms of natural persons do not require notification to the authority. This can be the case if the personal data was already made public or if encrypted information was leaked but the confidentiality of the key remained intact.

When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller must also notify the individuals whose personal data was impacted by the breach. The threshold for communicating a breach to individuals is higher than the threshold to notify a breach to the supervisory authorities. The communication of a breach to individuals must be made 'without undue delay'. A prompt communication will allow the individuals to protect themselves against the possible negative consequences of the breach.

The communication to individuals must contain at least the same information as the information provided in the notification of the breach to the supervisory

authority. The controller preferably also provides advice to the individuals on how to protect themselves against possible adverse consequences of the breach.

The breach must be communicated to the individuals directly. In order to do so, controllers are encouraged to use dedicated messages that do not contain any other information, such as newsletters, commercial updates or other regular means of communication.

Communicating the data breach to individuals is not required if:

- The controller has implemented appropriate technical and organizational protection measures hat render the personal data unintelligible to any person who is not authorized to access it (for example, encryption);
- The controller has taken subsequent measures ensuring that the high risk to the rights and freedoms of data subjects are no longer likely to unfold; or
- If a direct communication would require a disproportionate effort, in which case a public communication or similar measure to effectively inform the individuals, is sufficient.

Of course, a re-evaluation over time is advisable as circumstances change and notification might become necessary after all. Even if an organization would decide not to notify the data subjects involved, the authority can still require it do so if the breach is likely to result in a high risk for individuals.

The Working Party generally advises controllers becoming aware of a breach, not only to restrain the incident but also to assess the risk that could result from it. This will help the controller to take effective steps to restrain and address the breach, to decide whether or not notification is required to the authority and, if necessary, to the individuals involved. In case of doubt, the controller is encouraged to notify the supervisory authority.

In line with the accountability principle, the Working Party emphasis the obligation to also keep an internal register of all data breaches, regardless of their risk level as well as any reasons and justifications for not notifying any supervisory authorities or communicating a data breach to individuals.

Privacy Shield survives first joint annual review

As elaborated in Privacy Flash issue 14, the Privacy Shield was established in August 2016, following the demise of the Safe Harbor framework as a result of the famous Schrems case. The Privacy Shield aims at providing an adequate level of protection of the fundamental rights of any individual in the European Union whose personal data is transferred to the United States. Additionally, it aims at enhancing legal certainty for businesses relying on transatlantic data transfers.

The Privacy Shield includes an annual review mechanism, obliging the Commission to assess its functioning on a yearly basis. On 18 October 2017, the first annual report was published. Overall, the Commission is pleased with the efforts put forward by the US authorities stating that "*the United States continues to ensure an adequate level of protection for personal data transferred under the Privacy Shield from the Union to organizations in the United States*". However, the Commission identifies room for improvement in the area of the Shield's practical implementation. Therefore, the report contains a few recommendations.

A first recommendation addresses the certification mechanism for United States' companies. Companies who have started but not yet finalized their certification procedure, are allowed to publicly refer to their Privacy Shield certification. According to the Commission, this may mislead EU individuals, as these companies have not yet officially obtained their certificate. In addition, the Commission considers that this practice undermines the credibility of the Privacy Shield framework and ought to be prohibited. In their opinion, the US Department of Commerce should also proactively search for false claims of participation in the Privacy Shield.

A second topic for improvement relates to Privacy Shield compliance monitoring. Once certified, companies ought to be subject to regular compliance checks. This would allow the US Department of Commerce to identify possible compliance issues and to assess whether more systemic deficiencies in the functioning of the framework ought to be addressed.

Further recommendations include the strengthening of the efforts made to raise awareness regarding the Privacy Shield framework. The Commission praises the efforts already made by the US Department of Commerce and the EU Data Protection Authorities. However, more efforts are required in the field of informing EU individuals about exercising their rights and the possibility to lodge complaints. In order to fulfil this goal, enhanced cooperation between enforcers is inevitable.

Soon after, the Article 29 Working Party issued its own Report on the first annual Privacy Shield review. The Working Party welcomes the progressive efforts made by the US authorities to set up a comprehensive procedural framework supporting the operation of the Privacy Shield. However, it also raises several concerns, which only partially overlap with the areas of improvement identified by the Commission. The WP 29 expects all of its concerns to be addressed at the very latest during the second joint review of Privacy Shield. If not, its members, i.e. national data protection authorities, will take appropriate action including bringing the Privacy Shield before national courts to obtain a reference to the Court of Justice for a preliminary ruling.

Although these concerns partially overlap with the Commission's findings, the Working Party emphasizes the lack of an independent Ombudsperson and the further development of rules of procedure as key focus points.

CNIL publishes guidance for processors

On 29 September 2017, the French Data Protection Authority (CNIL) published guidance on the data processors' obligations under the new General Data Protection Regulation. This guide uses a FAQ format to provide practical advice to data processors on how they are to comply with their obligations.

The CNIL provides a clarification on the concept of a data processor and provides some practical examples of organisations that may be categorized as processors (e.g., SaaS vendors, marketing and communications agencies with access to personal data, etc.) and other organizations that may not be considered as processors (e.g., software publishers, manufacturers of materials). Reference is being made to the criteria provided in the Working Party 29 Opinion 1/2010.

Next to that, the guidance highlights all of the upcoming changes under the GDPR relating to direct obligations imposed on processors:

- Transparency and traceability: processors have, for example, the obligation to set a contract with the controllers, to obtain the controllers' prior authorization to engage any subprocessor and to keep a record of all processing activities.
- Privacy by design and privacy by default: processors should put in place all the necessary measures to ensure that the data processing activity complies with the GDPR's requirements. This implies that all requirements and principles have to be taken into consideration at the initial stage of a project and that e.g., only data that are necessary for the purpose of the operation are processed.
- Obligation to ensure the security of the data processing: this includes the obligation to notify the controller in case of data breaches.
- Obligation to alert, assist and advise the controller: processors have to inform the controllers when its instructions are unlawful, provide reasonable assistance to controllers to respond to requests from data subjects and to assist the controllers to comply with their obligations regarding data security, data breach notifications, and data protection impact assessments.

For these purposes, the CNIL's guidance has developed a three-step checklist, helping processors to fulfil these obligations:

- Assess if a DPO should be appointed;
- Analyse and revise current data processing agreements. The Guide includes template data processing clauses that can be used until standard clauses have been adopted by the European Commission;
- Establish and keep an inventory with all data processing operations.

Furthermore, the guidance provides more explanations on the processors' obligations when relying on subprocessors, their responsibility in case of data breaches, their role in the context of a DPIA, etc. The CNIL concludes by summarizing several situations which could lead to administrative sanctions under the GDPR.

Irish DPC issues guidance on e-receipts

The Irish Data Protection Commissioner has issued guidance for retailers on the use of e-receipts for marketing purposes. A growing number of retailers offer their customers, at the moment of purchase, the option to receive a receipt via e-mail – an e-receipt. The customer must be informed, at the moment their e-mail address is being requested, that it will be used to provide them with an e-receipt. Audits by the Commissioner have shown that many retailers subsequently use the collected e-mail addresses to send direct marketing communications as well.

Customers have not necessarily consented to this additional use of their e-mail address. In fact, retailers are not allowed to use this contact information for marketing purposes unless they have given the customer the choice to "opt-out". The Irish DPC states more specifically that contact information collected in the context of the sale of a product or service (including the right to send e-receipts), may only be used for direct marketing by e-mail, if the following conditions are met:

- The product or service being marketed is similar to that bought by the customer at the time the retailer collected the contact details;
- The customer was given the chance to object to the use of his contact information for marketing purposes, at the time the information was collected;
- The customer is given the right to object to further messages, each time a marketing communication is sent out;
- The initial sale occurred not more than a year prior to the sending of the marketing e-mail, or – if appropriate – the details were used to send an electronic marketing message during that 12 month period.

If e-mail addresses are actually gathered solely for the purpose of providing e-receipts, the retailer should still draw up a retention period for the retention and deletion of these e-mail addresses.

In Ireland, each unsolicited marketing email can lead to a fine of up to €5.000 on summary conviction. When convicted on indictment, the fines can even range up from €50.000 for a natural person to €250.000 for a corporate body.

Uber data breach

In October 2016, Uber suffered a massive data breach affecting about 57 million of its users, both drivers and riders. Uber did not report the incident to regulators at that time nor to the affected customers. Instead, it paid $100.000 to the attackers to keep the breach a secret.

According to Uber, two individuals outside the company have inappropriately accessed user data stored on a third-party cloud-based service that Uber uses. The attackers were able to gain access to a private GitHub coding website that Uber software engineers used. The hackers took login credentials from the site to access the company's massive data store. Allegedly, no trip location history, credit card numbers, bank account numbers, social security numbers or dates of birth were downloaded. The attackers did however gain access to:

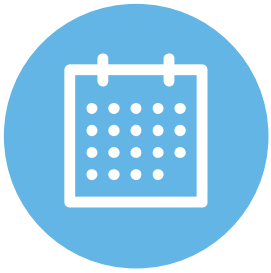
- The names and driver's license numbers of around 600.000 drivers in the US;
- Personal information of 57 million Uber users around the world (including the drivers), including names, email addresses and mobile phone numbers.

The news about this data breach incident comes very shortly after Uber settled an agreement with the FTC (American Federal Trade Commission). Following several complaints from the Commission, Uber supposedly agreed to implement a comprehensive privacy program and to obtain regular, independent audits to settle the charges. The FTC accused Uber of deceiving its consumers by failing to monitor employee access to consumer personal information and by failing to reasonably secure sensitive consumer data stored in the cloud.

Dara Khosrowsashi, Uber's new CEO, has addressed the breach on the Uber website. Evidently, the breach occurred when Uber was still steered by its former CEO, Travis Kalanick. Uber now states to have taken several measures following this breach, such as:

- Seeking the assistance of a cybersecurity consultant and former general counsel of the NSA to guide and structure the Uber security teams and processes going forward;
- Notifying the drivers whose driver's license numbers were downloaded and providing them with free credit monitoring and identity theft protection;
- Notifying the regulatory authorities;
- Monitoring the affected accounts and flagging them for additional fraud protection.

Conferences



European Privacy Academy

Deloitte Gateway Building, Brussels Airport, Belgium, 26 February – 1 March 2018
http://www.europeanprivacyacademy.com/

The European Privacy Academy is a unique training, knowledge and networking centre, focused on practical day-to-day management of privacy challenges. It provides both an on-campus data protection officer course as well as on-campus or in-house department-specific data protection training during which attendees learn to efficiently manage privacy and security in an integrated risk-based manner.