Deloitte.

dReport: January 2019

Check out our regular Legal news newsletter.

GDPR in practice or 11 pieces of advice and recommendations to get the better of the personal data protection regulation

The General Data Protection Regulation or the GDPR was one of the most discussed topics last year. Its compulsory implementation in practice, which occurred in May 2018, was preceded by stormy debates, careful preparations of stakeholders and uncertainty about the practical consequences the regulation would produce. At a business breakfast held at the end of the last week, we assessed the first six months of the GDPR's implementation. We have selected the 11 most interesting pieces of advice and recommendations to help you find out whether the steps you have taken are in line with the regulation and what to do to achieve compliance.

1. Initial analysis

Obtaining all relevant information from companies is the first important step for accurate GDPR implementation. "We meet with major companies, talk to them and inquire what data they collect, for what purpose and in what systems", explains Ján Kuklinca, attorney-at-law at Deloitte Legal, and adds: "Small companies sometimes prefer a more economical way of status mapping, such as completing questionnaires. The third option is a combination of the two previous alternatives". Based on the data collected, Deloitte provides its clients with its recommendations.

2. Documentation for individuals should be written understandably

Texts are often produced by lawyers, sentences are complex and long, sometimes taking ten lines. However, firms should try to express themselves briefly and provide understandable information. "A summary should be provided at the beginning to make it clear that a company wants to be transparent. Try to see yourselves in an addressee's place and make the information understandable for him or her. Images and pictograms are also recommended. When providing their consent, people should know what they are signing up to", advises Martina Heřmanová, attorney-at-law at Deloitte Legal.

3. Documentation distribution to separate categories

"We recommend dividing information on processing into separate categories of individuals, namely information for customers, suppliers and HR", says Ján Kuklinca. The format of any privacy policy (personal data protection principles/information) should always be adjusted depending on how a company communicates with the individual groups and when it contacts them.

4. Records on processing activities

Today, any controller should have a document containing records on personal data processing activities. Its form is not strictly defined; it depends, for example, on the size of the company. It is important that all activities performed by the company be recorded in the document. "The Office for Personal Data Protection considers such a document to be a 'Holy Grail': it is likely to be the first document to be examined during an audit", says Martina Heřmanová and highlights the need to update the records on an ongoing basis.

5. Controller's internal regulations

It is crucial for any controller to have internal regulations in place to treat personal data. All employees should know what to do with personal data, whom to address if something is not clear in a relevant company or how to solve any security incidents. "We also recommend introducing shredding and filing guidelines and plans", states Martina Heřmanová and adds: "A number of companies lack these documents although the rules on destroying, archiving and administering physical and data documents had been required by Czech legal regulations before the GDPR's effective date".

6. What other organisational measures to introduce?

It is well advised to arrange e-learnings or training sessions for employees to be aware of all measures relating to the GDPR. Setting up IT systems to facilitate the GDPR-related processes is another recommended step. Firms also appoint a Data Protection Officer (DPO) or a contact person. "In our experience, it should be a person knowledgeable of what is going on in a company and having unlimited access to records on processing activities rather than just a formally appointed individual", stated Ján Kuklinca.

7. Consent with personal data processing

Under certain circumstances, consents are necessary measures required for the company to process personal data. Before, consents with personal data processing were part of contracts. This approach is, however, not considered to be a voluntary consent. Consents thus cannot be part of contracts or business terms, they should always be provided separately. This relates to another topic, which is collecting excessive consents, ie even if there are other legal grounds, such as processing required to perform a contract, meeting statutory requirements or legitimate interest of a controller. "Obtaining consents should be the last option", recommends Martina Heřmanová, attorney-at-law at Deloitte.

8. Position of a third party processor

A processor is simply an entity to which the controller provides personal data to process it depending on the controller's authorisation and instructions. The relation between a controller and a processor is subject to a contract under Article 28 of the GDPR. "We often see that our clients have concluded this type of contract with another controller, which is not correct. The two entities provide data to one another but each controls it independently", explains Martina Heřmanová.

9. Call records

When recording calls, there are various situations. The first one is simply a call to an advice line. Although the call is recorded there is no systematic approach of searching the information on who the caller was and the tape is not used to improve the quality of services. This is not personal data processing and there is no need to obtain any consent with personal data processing. The second situation includes calls in which a company (often a financial institution) identifies the calling person by a phone number and allocates the record to that person. This is personal data processing and the issue whether and how to obtain the calling person's consent should be solved. The consent should be received through an active step taken by the calling person, such as pressing a button.

10. Cookies

In order to solve cookies under the Czech legal environment only, the Office for Personal Data Protection has stated that it is sufficient to inform on a company's website that the relevant company uses cookies and how it does so. However, if the company's owner is from abroad, this approach might not be sufficient. An active consent with the use of cookies is usually required.

11. Selection procedure

In practice, employers often keep CVs of job applicants who were not successful in selection procedures for an excessive period and address them to offer them other jobs. If a company wants to keep a CV in its records it should obtain an applicant's consent first.

Google Receives a Fine of EUR 50 Million for Violating the GDPR

On 21 January 2019, the French equivalent of the Czech Office for the Protection of Personal Data (the "OPPD"), Commission nationale de l'informatique et des libertés (the "CNIL"), imposed a fine of EUR 50 million on GOOGLE LLC for violating the General Data Protection Regulation (the "GDPR"). The fine was imposed for lack of transparency in processing personal data, for insufficiently informing data subjects, and for invalid consents relating to the personalisation of advertising.[1] This is by far the greatest sanction imposed to date since last May, when the Regulation came into effect.[2]

The CNIL started to look into the case at the instigation of two privacy rights organisations as the authority in Ireland, where Google's European headquarters are based, had insufficient decision-making powers.[3] the complaint was filed on behalf of several thousand Android users on the very day that the GDPR became effective.[4]

Google failed to provide information to users with sufficient transparency

The CNIL found that the information provided by Google to users was not sufficiently easy to access. The information that must be provided pursuant to the GDPR (eg, the processing purpose or period of storing personal data) was diluted across several documents that required five to six clicks or other actions if the user wished to obtain full information. The CNIL also concluded that the processing purposes as stated by Google were too vague and did not adequately explain the legal grounds for processing. Therefore, users may not have had clear information as to whether the processing was based on their consent or the protection of Google's legitimate rights.

The CNIL found the "pre-ticked" consents to be invalid

The consents which Google was granted for the purposes of ads personalisation were found to be invalid for two reasons. Firstly, as the information was fragmented, it was impossible for users to trace the actual scope of services and applications using the data and were thereby insufficiently informed.

Secondly, the consents were neither sufficiently clear nor specific (granted for each individual purpose). For users to be able to create an account, they had to tick off that they agreed with the terms of use and personal data processing "described above and explained in the personal data processing rules". In doing so, users gave their consent to all purposes such as ads personalisation or speech recognition. Neither was Google saved by the fact that it subsequently enabled users to click on the pre-ticked consent with ads personalisation. According to the CNIL, the correct treatment would be, for example, for the user to actively mark an empty field.

The amount of the fine was justified by a breach of basic principles

The CNIL justified the amount of the fine by the severity of the breach, which was related to the basic principles on which the GDPR is founded: transparency, information and consent. In addition, the CNIL stated that the breach had been committed on a large scale until the present day; therefore, it was not a one-off breach. The fact that Google's economic model is partially based on ads personalisation was also weighed against Google by the CNIL, therefore it was "of its utmost responsibility to comply with the obligations on the matter".

Last year, the Czech OPPD announced that until the GDPR adaptation act was adopted, it primarily wished to raise awareness of the GDPR rather than impose sanctions.[5]

However, as the Regulation is applied in the whole EU in the same manner[6], there is no reason to assume that the OPPD's assessment of the case would differ from that of the CNIL in the event of such extensive and systemic misconduct.

Matúš Tutko
mtutko@deloittece.com

---

1. The CNIL's restricted committee imposes a financial penalty of 50 Million euros against GOOGLE LLC [online, quoted on 23 January 2019]. Available on the following website: https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc.
2. FORNEY, Mitchel. GDPR Fine Tracker – an Ongoing, Always-Up-To-Date List of Enforcement Actions [online, quoted on 23 January 2019]. Available on the following website: https://alpin.io/blog/gdpr-fines-list/.
3. These were the French organisation La Quadrature du Net (https://www.laquadrature.net/en/about/) and the Austrian organisation noyb (https://noyb.eu/concept/).
4. FOX, Chris. Google hit with £44m GDPR fine over ads [online, quoted on 23 January 2019]. Available on the following website: https://www.bbc.com/news/technology-46944696.
5. Do not fear GDPR-related sanctions, the Office wishes to explain things first [online, quoted on 23 January 2019]. Available on the following website: https://www.podnikatel.cz/clanky/pokut-u-gdpr-se-zatim-nebojte-urad-chce-zprvu-hlavne-vysvetlovat/.
6. Barring minor departures stipulated by national legislation.

Deloitte.