THE PRIVACIST - VOLUME 1

Date: 3 October 2019

Global Data Protection, Privacy, and Security Alert

By: Claude-Étienne Armingaud, Pamela J. Garvie, Dr. Thomas Nietsch, Mark H. Wittow, Etienne Drouard, Violaine Selosse, Francesca M. Cardillo

BREXIT: DEAL OR NO-DEAL? DATA IS THE QUESTION

With the Brexit deadline looming ahead on 31 October 2019, the situation seemingly reaches new levels of uncertainty every day. Last week, the U.K. Supreme Court's eleven judges unanimously ruled that Prime Minister Boris Johnson's decision on 9 September 2019, to prorogue Parliament was “unlawful and void.” Parliament will therefore carry on its Brexit discussions...with now only thirty days left to finalise a deal. Although Parliament, while still in session, passed a law to extend the Brexit deadline, such an extension would still require approval by the EU.

So how should companies prepare, on either side of the Channel (and beyond), in the coming months for the more-likely-by-the-day-scenario of No-Deal?

On Brexit day, the EU GDPR will be incorporated into U.K. law by the British European Union (Withdrawal) Act 2018 and will therefore remain applicable *mutatis mutandis* in the U.K. In particular, this will allow data transfers from the U.K. to the EU to carry on as usual, unrestricted and without need for stakeholders to take any specific measures. In addition, the U.K. supervisory authority (ICO) has published extensive guidance regarding a No-Deal Brexit, prefiguring the continuity of the EU regulations into the U.K. national laws: the EU's Adequacy decisions, binding corporate rules, standard contractual clauses, Court of Justice of the European Union decisions and even the EU Privacy Shield will still be recognized by the U.K. Consequently, U.K. companies which had already implemented GDPR compliance measures for data transfers (as they should have since 25 May, 2018) will not need to take any further action.

However, the U.K. will still become a “third country” for the purposes of GDPR, thereby requiring adequate safety measures to be put in place prior to any transfer to the EU. The U.K. government aims to obtain an “adequacy decision” from the European Commission, which would allow for the free transfer of data from the EU to the U.K., following in the footsteps of Japan, South Korea and India (the last two currently seeking EU's approval). However, the process and discussions for obtaining such an adequacy decision can last for up to 18 months, and the EU has stated that the process cannot start until the U.K. officially becomes a “third country,” i.e. on 31 October 2019 at the earliest.

In the meantime, companies will therefore need to consider alternative mechanisms, which need to be in effect by 1 November 2019. These could consist in the following:

- Binding Corporate Rules represent a lengthy and costly process, especially considering that the rules have to be validated by the national supervisory authority;
- Codes of conduct or certification mechanisms, which would be circumstantial (varying according to industry standards) and have yet to be issued or authorized by national supervisory authorities (following consultation of the European Commission);
- Standard contractual clauses (as approved by the European Commission), which seem to be the only viable option considering how little time is available.

Although it is clear that a No-Deal Brexit will be more cumbersome for EU entities transferring data to the U.K. than vice-versa, we should bear in mind that U.K. companies must likewise implement mechanisms for data transfers to "third countries," although any existing arrangements will transitionally be recognized by the U.K. In the specific case of the United States of America, the Privacy Shield will continue to apply to restricted transfers from the U.K. to the United States of America. However, U.S. organizations participating in the Privacy Shield will need to expressly state in their public commitment to comply with the Privacy Shield that those commitments apply to transfers of personal data from the U.K.

With the growing importance of a data driven economy in a global setting, any hard stop on the flow of data between stakeholders would likely bring dire consequences, including the potentially huge fines in case of noncompliance.

CJEU ISSUES LONG-AWAITED DECISION ON COOKIES

On 1 October 2019, the Court of Justice of the European Union (the CJEU) issued its long-awaited decision about the cookies consent validity and the information that needs to be provided to data subjects prior to setting cookies on their terminals. The CJEU ruled in Case C-673/17 that consent could not validly be obtained through using pre-ticked checkbox.

German company Planet49 had organized online promotional games on its website. In order to participate, the users had to fill in a form, which contained a cookie provision with a checkbox containing a pre-selected checkbox. In order to oppose to cookies, the user had to deselect the option. By clicking on the hyperlink "You can read more about this here," the user was redirected to the cookies policy, which did not include any information relating to (i) the retention period applicable to the cookies, or (ii) third parties' access to such cookies. The policy also specified that the advertising partners did not receive any personal data of the tracked users.

Asked by the Federal Court of Justice of Germany, the CJEU stated that:

- the wording "given his or her consent" had to be interpreted literally and thus, required an active behavior or a clear affirmative action from the user. Such a requirement was therefore incompatible with the use of pre-ticked checkboxes, nor could it be inferred from the mere action of filling an online form;
- the wording of the ePrivacy Directive 2002/58 did not operate any distinction on the "storage the information" on the basis of the data being personal or not. Thus the provisions related to consent shall be interpreted indifferently according to whether the processed data is personal or not; and
- information provided to data subjects had to remain clear and comprehensive. Even though the duration of the cookies is not explicitly mentioned in the ePrivacy Directive, it must be included in the notice

provided on the website (or at least the criteria used to determine such duration). Finally, for the third parties' access to cookies, third party partners being considered as “recipients,” their list should be provided to the user as a part of the service provider's legal obligation arising out of Articles 13 and 14 GDPR.

POLISH DPA'S LARGEST FINE FOR A DATA BREACH

On 10 September 2019 the Polish Data Protection Authority (UODO) issued a fine of EUR 645.000 against an online retail company morele.net (the “Company”) for insufficient security and organizational measures violating data confidentiality and integrity principle described in Article 5.1.f GDPR, and its obligations as data controller arising from Articles 24, 25 and 32 GDPR. The insufficient security measures resulted in data theft of over 2.2 million natural persons registered in the databases of 11 online retailers and significantly increased risks of identity thefts.

The first data breach occurred in November 2018, when phishing emails were sent to customers requesting that they proceed with a PLN one payment via an SMS gateway. Few days later, the Company received an anonymous letter informing them about the database theft. The local police has been informed and an investigation ensued. A second similar data breach occurred a month later, where hackers acquired personal data relating to the identity and contact details (name, surname, email address, phone number), but for 35,000 of customers, the data breach revealed also their financial reports, national identity number (PESEL) and ID/passport numbers.

UODO assessed that the technical security measures were insufficient, the authentication methods used by the Company were not secure enough, and the additional security solutions had only been implemented further to the data breach. Moreover, the organizational security measures were also unsatisfactory as, for instance, no action plan in case of an abnormal behavior on the Company's website had been implemented. The recommendations of an external IT audit services provider were considered inadequate by UODO, since they were not compliant with the updated ISO quality norms such as PN-EN ISO/IEC 27001:2017-06. According to UODO, Article 32.1 GDPR mandates that data controllers ensured that their security solutions were up to date with then-current standard, especially ISO norms. UODO also cited standards included in the guidelines prepared by the international cybersecurity organizations such as OWASP, NISP or ENISA.

Moreover, UODO found that the Company did not present the sufficient evidence of the customers' consent to the processing of their data, as it was unable to document how it effectively processed the users' data in a legitimate way, thereby also breaching GDPR's accountability principle.

While the data breach had not stemmed from any intentional act of the Company, as a data controller, it had to bear the full responsibility for the incident. Nonetheless, when pronouncing the fine, UODO took into account the mitigating circumstances: the fact that the Company willfully and duly cooperated with the authorities, implemented the necessary measures to end the data breach and has not been previously sanctioned.

The largest UODO's fine to date underlines the importance for data controllers to implement appropriate and up-to-date security measures not only to remedy but also, to prevent potential risks associated with data breaches.

LIECHTENSTEIN DPA PUBLISHES GUIDANCE ON THE ROLE OF DATA CONTROLLERS

European Economic Area microstate Liechtenstein published its guidance on the role of data controllers drawing on the 2010 guidelines from the European Data Protection Board's predecessor, the WP29, and taking into account the latest developments by the European Court of Justice (*Fashion ID*, C-40-17 - 29 July 2019 and *Wirtschaftsakademie*, C-210-16 - 5 June 2018).

While, like GDPR, the guidance does not explicitly state that entities which process the similar data for independent purposes (i.e. “co-controllers” as opposed to the explicitly defined “joint controllers”) must enter into a written agreement detailing each counterpart's prerogatives, such document would seem the only way to evidence their respective roles, as part of the accountability framework set forth by GDPR.

BAVARIAN DATA PROTECTION COMMISSIONER'S GUIDANCE ON “MANIFESTLY UNFOUNDED” OR “EXCESSIVE” DATA SUBJECT ACCESS REQUESTS

The *Bayerische Landesbeauftragte für den Datenschutz*, the competent data protection authority for the public sector in Bavaria, published its guidance on how to assess the “unfounded” or “excessive” character of data subject access requests (DSAR). While limited to the public sector, its guidance sheds additional light on how to address DSARs.

Indeed, since GDPR entered into force, DSARs have been mostly used by data subjects in order to exercise their rights, but also verify that the processing activities of data controllers had been implemented in compliance with the regulation. However, more and more DSARs are now also used in order to (i) disrupt the legitimate activities of companies or (ii) obtain elements unrelated with data protection principles (e.g. evidence gathering in the context of litigation).

The Bavarian guidance highlights the exceptional nature of a refusal to process a DSAR, which must be assessed *in concreto*, notably if it is apparent that the data subject is only seeking to abuse the resources of the data controller or to sanction the data controller on a non-GDPR related ground.

US CONGRESS PUSHES FOR PRIVACY LEGISLATION AHEAD OF CCPA

Those hoping California lawmakers might delay or significantly narrow the scope of the California Consumer Privacy Act (CCPA) before it takes effect on 1 January 2020, were disappointed earlier this month, when the legislature adjourned without making major changes to the state's landmark privacy law. The legislature's adjournment increases the urgency of efforts to enact privacy legislation at the federal level, where Congress is quickly running out of time to do something before the end of the year.

Given the broad scope of the CCPA (described in our client alerts here and here) and the federal proposals under discussion, the outcome of this sprint to the finish line matters to any organization that collects, uses, processes, stores, or shares personal information. If efforts at the federal level fall short, organizations need to be prepared to comply with the CCPA, including the technical amendments that passed in the recently concluded legislative session.

You can read full analysis of the current state of play and what clients can expect heading into year-end on our alert here.

KEY CONTACTS

CLAUDE-ÉTIENNE ARMINGAUD
PARTNER

PARIS
+33.1.58.44.15.16
CLAUDE.ARMINGAUD@KLGATES.COM

PAMELA J. GARVIE
PARTNER

WASHINGTON DC
+1.202.661.3817
PAMELA.GARVIE@KLGATES.COM

DR. THOMAS NIETSCH
PARTNER

BERLIN
+49.30.220.029.408
THOMAS.NIETSCH@KLGATES.COM

MARK H. WITTOW
PARTNER

SEATTLE
+1.206.370.8399
MARK.WITTOW@KLGATES.COM

