ACCOUNTANCY EUROPE.

UPDATE

EU DATA PROTECTION RULES

HIGHLIGHTS

- The European Commission calls for more awareness raising, particularly for SMEs
- Different EU actors have published guidance to facilitate GDPR compliance
- Data transfers to the US have come under pressure (again)
- Brexit will impact data transfers between the EU 27 and the UK

INTRODUCTION

This update provides an overview of the latest developments on the EU General Data Protection Regulation (GDPR). To this end, it will start with the Commission's stock-taking exercise of the GDPR implementation and provide an overview of the official available guidance. The third part will focus on data transfers to third countries. This is the main part of this update given the many developments in this field. Finally, a brief description is given of the review of complementary EU privacy legislation.

This update complements the factsheet *What do the new EU data protection rules mean for you?*

ARE WE THERE YET?

On 24 January 2018, the Commission published a stock-taking exercise of the preparatory work to ensure GDPR application.

The Commission calls on national data protection authorities to increase their awareness raising activities, in particular regarding SMEs. To help Member States, the Commission has set aside €3.7 million to train enforcement authorities and help them support businesses to achieve GDPR compliance.

Moreover, the Commission concluded that Member States need to make sure, the regulatory framework is in line with the GDPR. According to the Commission, only Austria and Germany have so far managed to adjust their national rules. Nonetheless, several Member States are currently in the process of discussing new draft laws.

In the coming months, the Commission will:

- monitor GDPR application and start infringement procedures against Member States if necessary (from 25 May)
- participate in awareness raising exercises, e.g. events at national level

GUIDANCE

EUROPEAN COMMISSION

The Commission published the following guidance to raise awareness about the GDPR:

- Infographic: What your SME must do
- FAQs

The infographic gives a general idea of what the GDPR is about. It does not answer practical questions.

The FAQs are more hands-on and provide answers to questions such as: “Does my company/organisation need to have a Data Protection Officer (DPO)?”, “What is a data controller or a data processor?” or “For how long can data be kept and is it necessary to update it?”. Some of the answers contain examples to help the reader understand how the legislation is applicable in practice.

The Commission intends to update its FAQ based on feedback it receives. So it is worth to return to the page or submit a question.

EU PRIVACY WATCHDOG

The so-called Article 29 Working Party (WP29) unites all national data protection authorities, the European Commission, and the European Data Protection Supervisor. It is one of the key data protection actors at EU level. It regularly produces opinions and guidance on data protection legislation. Member States will have to repeal or bring into line their national guidelines with those from the WP 29.

WP 29 guidelines clarify different GDPR concepts, including the Data Protection Officer, Data Protection Impact Assessment, or the use of ‘consent’ to process data. They are more detailed and technical than the Commission’s guidance.

We can expect more guidance to come from the WP29. For example, on when businesses need to maintain a record of processing activities. This is said to address specific SMEs needs.

Once the GDPR starts applying, WP29 will be transformed into the European Data Protection Board. It will then play a crucial role to ensure a uniform application of the GDPR across the EU. It will do this by producing further guidance, settling disputes between countries regarding cross-border processing of data, and provide opinions, for example on whether a proposed industry Code of Conduct is compliant.

TRANSFERS TO THIRD COUNTRIES

Personal data can only be transferred to countries outside the EU when the same level of data protection can be guaranteed. In practice, this means that either a country must have a similar data protection framework as the EU, or that data controllers must adopt certain measures to guarantee sufficient data protection.

The easiest way to transfer personal data outside the EU is when there is an ‘adequacy decision’. By adopting an adequacy decision, the Commission formally declares that it assessed that the data protection in a certain country is ‘adequate’. This means that data transfers can be made to such third countries without specific authorisation.

So far, the Commission recognised only a few countries as having an adequate level of protection. This includes: Andorra, Argentina, Canada (commercial organisations), Faeroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland and Uruguay.

Personal data can also be sent to a third country even if there is no adequacy decision. However, businesses will then have to adopt appropriate safeguards, such as binding corporate rules, standard contractual clauses, a code of conduct, or certification processes.

The following sections will look at recent and upcoming developments related to adequacy decisions.

FORTHCOMING ADEQUACY DECISIONS

Work is ongoing for an adequacy decision with Japan. European Commissioner for Justice, Věra Jourová, has expressed optimism to adopt such a decision by May 2018. However, this would mean that some fundamental differences between the EU and Japanese data protection need to be resolved.

Moreover, the Commission launched talks with South Korea in view of a possible adequacy decision.

Finally, the EU is engaging with key trading partners, notably in East and South-East Asia and Latin America, to explore the possibility to adopt adequacy decisions.

EUROPEAN ECONOMIC AREA

The Commission is working with the three European Free Trade Association (EFTA) members of the European Economic Area (EEA) to integrate the GDPR into the EEA agreement. After 25 May, personal data will only be able to flow freely between EU and EEA countries once this is done.

To recall, the EEA integrates Iceland, Liechtenstein, and Norway in the EU Internal Market. Relevant EU legislation becomes applicable to these countries by incorporating an EEA-relevant act into the EEA Agreement. Currently, the EEA Agreement covers the Data Protection Directive 95/46/EC and all related “adequacy decisions”.

US

The European Commission adopted a partial adequacy decision for the US: the EU-US Privacy Shield. It is partial because it only applies to US companies which voluntarily signed up to Privacy Shield and self-certified with its principles. Once they commit to comply with the requirements, these will become enforceable under US law.

As a result, the Privacy Shield only allows the transfer of personal data to the United States for companies that subscribed to the mechanism. You can find the list of these entities here. It is therefore important for practitioners that store their data in the US to verify whether their cloud service providers are on that list.

The Privacy Shield is contested because several actors consider that it provides inadequate protection for European personal data. It is therefore advisable for practitioners that store their data in the US to take this into consideration and to follow any relevant developments announced by the European Commission. When the European Court of Justice struck down the predecessor of the Privacy Shield, the Safe Harbour Agreement, it created major legal uncertainty for audit and accountancy firms that processed data in the US.

The main stakeholders on this issue are privacy NGOs, the WP29 and the European Commission.

NGOS

The Commission has the power to adopt adequacy decisions. However, the European Court of Justice has the power to strike down such decisions if it considers these are not respecting EU legislation.

Different NGOs have started proceedings against the Privacy Shield. For example, the Quadrature du Net, French Data Network, and Fédération des Fournisseurs d’Accès à Internet Associatifs have challenged the Privacy Shield for not respecting the Charter of Fundamental Rights of the European Union. These proceedings are ongoing. Moreover, Digital Rights Ireland has filed a legal challenge, claiming that the agreement provides insufficient privacy protection. However, the EU General Court ruled that the action was inadmissible.

WP29

The WP29 reviewed the EU-US Privacy Shield adequacy decision. It identified significant concerns and, therefore, calls for an action plan from the Commission and the US to demonstrate that these concerns will be addressed.

The data protection authorities provide 2 deadlines:

- 'prioritized concerns' need to be resolved by 25 May 2018, when the General Data Protection Regulation starts to apply
- other concerns need to be addressed by the second annual review of the Privacy Shield, which is expected for Autumn 2018

The data protection authorities will challenge the Privacy Shield in court if their deadlines are not met.

EUROPEAN COMMISSION

The Commission annually reviews the Privacy Shield. On 18 October 2017, its first review concluded that the Privacy Shield ensures an adequate level of data protection.

However, the report also highlighted that there is room for improvement. The Commission would work with the U.S. authorities on the follow-up of its recommendations in the following months. This follow-up is not going smoothly and is affecting the Commission's attitude towards the US and the Privacy Shield.

European Commissioner for Justice Vera Jourova warned on 5 March 2018 that the Commission will suspend the Privacy Shield if it is not fully implemented. She made this statement during an exchange of views with the European Parliament, which has previously published a report that is highly critical of the Privacy Shield.

CONCLUSION

While contested and criticised, the Privacy Shield is still in place. However, its position might come under increased pressure if WP29 and the European Commission find that it provides insufficient protection.

BREXIT

Brexit may have an impact on data processing practices of businesses across Europe. This includes EU27 accountancy practices which process personal data in the UK, for example when using a UK cloud service provider. Moreover, UK businesses will still be subject to the GDPR when they are active in the EU27 and thereby process personal data.

EU and UK authorities have in recent months tried to provide more clarity on what will happen after Brexit when it comes to data flows.

EUROPEAN COMMISSION

The Commission published in January an information notice to stakeholders about the legal repercussions of Brexit for compliance with the GDPR. Because of Brexit, the UK will become a 'third country' from 30 March 2019. From that moment, the GDPR's rules for transfer of personal data to third countries will apply to such transfers from EU Member States to the UK.

There are three ways to remain compliant in such scenario:

- The Commission adopts an 'adequacy decision' to allow the transfer of personal data
- Data controllers, e.g. accountancy practices, adopt appropriate safeguards such as standard data protection clauses or binding corporate rules
- Data controllers make use of 'derogations', which allow transfers in specific cases

This is subject to any transitional arrangement that may be contained in a possible withdrawal agreement.

It is therefore important for practitioners to contact their IT providers to verify whether their data is stored in the UK. If this is the case and depending on the outcome of the Brexit negotiations, they might be required to take additional safeguards to ensure GDPR compliance.

UK

The UK's department for Exiting the European Union has published a policy paper on *The exchange and protection of personal data - a future partnership*. The paper points out that new arrangements to govern the continued free flow of personal data between the EU and the UK will be needed. Moreover, it stresses that it is essential to avoid regulatory uncertainty for businesses and public authorities.

The UK, therefore, wants to explore "a UK-EU model for exchanging and protecting personal data, which could build on the existing adequacy model". For an adequacy decision to be adopted, the UK is dependent the Commission's assessment of its data protection framework. A positive assessment is more likely if the UK retains the EU's GDPR rules after Brexit.

Different stakeholders started speaking up about the future of data flows after Brexit. In a new report, techUK and UK Finance call on the UK and the EU to "*pursue mutual adequacy agreements to provide a legal framework for the movement of personal data between the two jurisdictions*". This is considered the most stable and legally secure option. Other options, such as standard contractual clauses, are considered "*narrow, unsuitable, burdensome and expensive*" and are seen as impractical for SMEs.

EPRIVACY: GUARANTEEING CONFIDENTIALITY IN COMMUNICATIONS

The GDPR protects only personal data. Other rules are applicable when it comes to non-personal data. These are currently under review.

The Commission proposed on 10 January 2017 a Regulation to enhance the protection of confidentiality of electronic communications. The proposal seeks to update the ePrivacy Directive in line with the latest technological developments. This includes extending the scope to new electronic communications services such as web-based email, Skype for Business, WhatsApp, or iMessage.

The proposal complements the GDPR by providing protection in situations outside the scope of the GDPR. For example, when a company emails non-personal information, such as trade secrets or bookkeeping figures. Consequently, the proposal is important to guarantee the confidentiality of companies' electronic communications.

The proposal can only become law when the European Parliament and the Council reach an agreement. However, discussions did not yet start between both institutions. While the Parliament adopted its position in October 2017, the Council is still debating the issue.