PENNINGTONS MANCHES COOPER

DOES THE GDPR APPLY TO MY BUSINESS?

The flowchart below provides guidance on how and when the GDPR applies to businesses outside the EU/EEA and attempts to distil the guidelines published by the European Data Protection Board into an easy-to-apply format. For multinational groups, the flowchart ought to be considered for each separate entity being assessed.

IS THE BUSINESS WITHIN THE SCOPE OF THE GDPR?

Question 1: Does the business have an establishment in the EU/EEA?

Guidance: Establishment implies the effective and real exercise of activity through stable arrangements.

Establishment is widely interpreted and is not limited to any particular legal form. It includes branches, offices, group companies, agents or other stable relationships within the EU/EEA.

The threshold for "stable arrangement" is quite low when the centre of activities of a controller concerns the provision of services online. In some circumstances, the presence of one single employee or agent may be sufficient to constitute a stable arrangement (amounting to an 'establishment'). Remember that this test applies to both controllers and processors.

The guidance recognises that "establishment" has limits, and states that, just because a non-EU entity's website can be accessed from the EU, this alone cannot lead to a conclusion that the non-EU entity has an establishment in the EU.

No → **Go to question 3**

Example: A US manufacturer has a subsidiary in France. The subsidiary is a stable relationship that exercises real and effective activity for the US company. Therefore, the US manufacturer has an establishment in the EU.

Yes ↓

Question 2: Is the business processing personal data in the context of the activities of an establishment in the EU/EEA (whether as a controller or as a processor)?

Guidance: Businesses based outside the EU/EEA but which have an establishment in the EU/EEA need to evaluate the extent of their GDPR obligations.

The relevant test is whether the business processes personal data **in the context of activities of an establishment in the EU/EEA.**

Penningtons Manches Cooper LLP is a limited liability partnership registered in England and Wales with registered number OC311575. It is authorised and regulated by the Solicitors Regulation Authority.

The EDPB guidelines suggest that the consideration of the following two factors may help in determining whether processing is being carried out 'in the context of its establishment' in the EU/EEA:

i. **the relationship between the business outside the EU/EEA and its local establishment in the EU/EEA – if the data processing of the business outside the EU/EEA is inextricably linked to the activities of the local establishment in the EU/EEA, this may trigger the application of GDPR, even if the local establishment is not actually taking any role in the data processing itself;**

ii. **revenue raising in the EU/EEA by the local establishment to the extent that such activities can be considered 'inextricably linked' to the processing of personal data taking place outside the EU/EEA and individuals in the EU/EEA.**

The guidance states that the meaning of "in the context of activities of an establishment" cannot be interpreted restrictively. The guidance does however acknowledge that some commercial activity led by a non-EU entity within the EU/EEA could potentially be "so far removed" from processing by an EU entity in a way that could be insufficient to bring the processing within the scope of EU data protection law.

The guidance recommends that non-EU/EEA businesses first determine whether personal data is being processed and secondly identify potential links between the activity for which the data is being processed and the activities of any establishment of the business in the EU/EEA. The GDPR applies to processing in the context of the activities of an establishment in the EU/EEA regardless of whether the processing takes place in the EU/EEA or not.

Yes

Processing is subject to the GDPR.

Go to question 3

Example: An e-commerce website is operated by a company based in the US. The personal data processing activities of the company are exclusively carried out in US. The US company has established a European office in Paris in order to lead and implement marketing campaigns towards European markets.

- The activities of the European office in Paris are inextricably linked to the processing of personal data carried out by the US e-commerce website insofar as the marketing campaigns aimed at EU markets serve to make the service offered by the e-commerce website profitable. The processing of personal data by the US company in relation to EU sales is inextricably linked to the activities of the Paris office's marketing campaigns in European markets. The processing activity by the US company will therefore be subject to the GDPR.

Example: A Chinese company has a subsidiary in Berlin which, being based in Germany, constitutes an establishment in the EU.

- The Chinese parent would be subject to the GDPR where its activities are related to the Berlin subsidiary. For example, if the Berlin subsidiary is raising revenue for the Chinese parent, the Chinese parent would be subject to the GDPR where it processes personal data related to this activity, even if the processing happens in China.

Penningtons Manches Cooper LLP is a limited liability partnership registered in England and Wales with registered number OC311575. It is authorised and regulated by the Solicitors Regulation Authority.

- The Chinese parent would not be subject to the GDPR if processing is not in the context of activities of an establishment in the EU. For example, the processing of employees of the Chinese parent based in China.

Business processes some personal data unrelated to an establishment in the EEA

Question 3: Does the business offer goods or services to individuals in the EU/EEA (or act as a processor for a business which does so)?

Guidance: Does the business target individuals in the EU/EEA by offering goods or services to them (irrespective of whether payment is made)? If so it will be subject to the GDPR.

This is a question of fact and circumstance. This criterion is aimed at activities that intentionally - rather than inadvertently or incidentally - target individuals in the EU/EEA.

If processing relates to a service that is only offered to individuals outside the EU/EEA but the service is not withdrawn when such individual enters the EU/EEA, the related processing will not be subject to the GDPR. A website alone is not enough to show that the business is targeting individuals in the EU/EEA. However, if the website can be viewed in a European language and ships goods or provides services to the EU/EEA, this evidences that the business does indeed target individuals in the EU/EEA.

Example: A Singaporean company offers a mobile news service based on users' preferences.

The service is offered exclusively to users located in Singapore who must provide a Singaporean phone number when subscribing. A Singaporean subscriber of the service goes to Greece on holiday and continues using the service.

Yes

Processing is subject to the GDPR.

Go to question 4

Penningtons Manches Cooper LLP is a limited liability partnership registered in England and Wales with registered number OC311575. It is authorised and regulated by the Solicitors Regulation Authority.

Although the Singaporean subscriber will be using the service while in the EU/EEA, the app is not directed at nor targets an EU/EEA audience so the processing of personal data by the app will not be subject to the GDPR.

Example: An Australian hotel has a website and markets to audiences in the EU/EEA. The website is available in English, French and Dutch and payments can be made in Euros and Pounds Sterling. As the hotel is targeting individuals within the EU/EEA, it will be subject to the GDPR.

No

Question 4: Does the business monitor individuals in the EU/EEA (or act as a processor for a business which does so)?

Guidance: Monitoring can include a variety of activities including tracking location (for example, through wearable and other smart devices), use of cookies, fingerprinting, personalised analytics, CCTV, market surveys and profiling. However, there must be some aspect of targeting. If the monitoring is not designed to capture individuals in the EU/EEA, it will not be subject to the GDPR.

Yes → **Processing is subject to the GDPR.**

Example: A US marketing company provides services to a Dutch business. Part of this service is analysing purchasing activities of the Dutch company's customers who are in the EU/EEA. As the US marketing company is monitoring the behaviour of individuals in the EU/EEA, it will be subject to the GDPR.

No

Business is not directly subject to the GDPR.

Penningtons Manches Cooper LLP is a limited liability partnership registered in England and Wales with registered number OC311575. It is authorised and regulated by the Solicitors Regulation Authority.

PENNINGTONS MANCHES COOPER

MY BUSINESS IS NOT AN EU/EEA DATA CONTROLLER. HOW ELSE MAY IT BE AFFECTED BY GDPR?

Even if a business is not directly subject to the GDPR as a controller, there are three key relevant scenarios where the GDPR can still have impact:

i. when a business outside the EU/EEA uses a data processor established in the EU/EEA;
ii. when a business acts as a data processor for a data controller subject to the GDPR;
iii. when personal data is transferred outside of the EU/EEA.

Question A: Does the business act as a data processor or use a data processor in the EU/EEA?

Guidance: A data processor is an entity that processes personal data on behalf of and on instructions from a data controller. It is the data controller who determines the purposes and means of processing. Where a processor is established in the EU/EEA and is processing personal data in the context of the activities of that establishment, it will be required to comply directly with the obligations imposed on processors by the GDPR. In particular, under the GDPR there must be a written contract between data controllers and their data processors. This contract must also include provisions that are prescribed by the GDPR. For example, a data processor must only act on the instructions of a data controller.

Common examples of these types of relationship include IT and payroll suppliers. Where a data controller subject to GDPR chooses to use a data processor located outside the EU/EEA, it will still be necessary for the controller to ensure by contract or other legal act that the processor processes the data in accordance with the GDPR. The processor located outside the EU/EEA will therefore become bound to comply with obligations derived from the GDPR which are imposed by controllers subject to GDPR by virtue of the contractual arrangements required under GDPR, even if it may not otherwise be directly subject to the GDPR.

Example: A processor established in Spain enters into a contract with a Mexican retail company, the data controller for the processing of its clients' personal data. The Mexican company is not directly subject to the GDPR. It has no establishment in the EU/EEA and does not sell to or monitor individuals in the EU/EEA. However, as the Spanish company is in the EU/EEA, it has an obligation to have a written contract with the Mexican company that includes provisions dictated by the GDPR.

Example: A German research institute conducts research into Inuit sign language. The research only concerns Inuit people in Greenland and the German institute uses a processor based in Canada. The Canadian processor is not processing the data of EU/EEA data subjects and would not be directly subject to the GDPR. However, the German controller needs to enter into a data processing agreement with the Canadian processor that includes the terms prescribed by the GDPR.

Penningtons Manches Cooper LLP is a limited liability partnership registered in England and Wales with registered number OC311575. It is authorised and regulated by the Solicitors Regulation Authority.

Question B: Does the business import or can it access personal data from the EU/EEA? And how will this be impacted by Brexit?

Guidance: The GDPR prohibits the transfer of personal data outside the EU/EEA unless there is a legal mechanism in place. The legal mechanism acts as a means to ensure that individuals retain certain rights in relation to their personal data even where it leaves the EU/EEA. If a business imports or can access personal data from the EU/EEA, even where it is an intra-group transfer, there must be a legal mechanism in place.

Common legal mechanisms

- ***Adequacy decision:*** This is a decision published by the EU Commission which states that the laws of a jurisdiction are of a high enough standard that no additional contractual requirements are needed to safeguard personal data. This is a very limited list of countries that includes: Andorra, Argentina, Canada (commercial organisations only), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland, Uruguay and United States (only for EU-US Privacy Shield transfers).

- ***Model clauses:*** These are standard clauses which can be appended (or signed separately) to permit transfer outside the EU/EEA. A key issue for businesses which are unfamiliar with these clauses is that they cannot be negotiated or amended. If the model clauses are changed, they no longer qualify as a de facto valid legal mechanism.

Brexit implications

The implications of Brexit for cross-border data flows will depend on the shape of Brexit resulting from the Brexit negotiations. However, businesses can make preparations in the following areas.

EU/EEA controllers / processors transferring personal data to the UK

Assuming that the UK is not in the EEA post-Brexit, then the UK will become a 'third country' for the purposes of GDPR. Post-Brexit this means that those ***in the EU/EEA wishing to transfer personal data to the UK will, unless and until the UK receives an adequacy decision, need to put in place one of the safeguards set out in the GDPR or rely on one of the permitted derogations***.

The UK government is currently negotiating with the EU on the post-Brexit model for cross-border data flows. The UK is seeking a bespoke data protection agreement with the EU as a preferred alternative to an adequacy decision. As the negotiations currently stand, however, a standard adequacy decision seems the most likely outcome for the UK.

The UK government has indicated that its priority is to ensure that there is no risk of a gap in provision for transferring data between the EU and UK once the transition period ends on 31 December 2020.

Penningtons Manches Cooper LLP is a limited liability partnership registered in England and Wales with registered number OC311575. It is authorised and regulated by the Solicitors Regulation Authority.

Given that the Data Protection Act 2018 enshrines GDPR standards in UK law, it seems likely that the UK would be granted adequacy but this is by no means certain.

The UK's immediate priority is to obtain concrete assurances from the EU that data will be able to flow between the UK and the EU after December 2020 on the same terms as now. Beyond that, the UK will likely seek to negotiate a bespoke agreement with the EU to allow much closer co-operation in data protection and data sharing.

Extra-territorial effect of EU GDPR

This will **affect UK** entities as well as non-EU/EEA entities. **UK businesses may directly need to comply with the EU GDPR even after Brexit by virtue of the extra-territorial effect of the GDPR, in respect of and to the extent that they directly offer goods or services to EU residents or monitor their behaviour within the EU.**

UK controllers which have an establishment in the EEA, customers in the EEA or monitor individuals in the EEA will therefore need to be mindful of this. The EU GDPR will still apply to this processing but the way UK controllers interact with European data protection authorities will change. The UK controller is also likely to have to appoint an EU/EEA representative under the EU GDPR.

UK GDPR

Although the EU GDPR will no longer be law in the UK when it exits the EU, the UK government intends to write the GDPR into UK law, with the necessary changes to tailor its provisions for the UK (the 'UK GDPR'). This will sit alongside an amended version of the Data Protection Act 2018 and require UK controllers and processors to effectively comply directly with GDPR standards by virtue of UK domestic law rather than under the EU GDPR itself.

Extra-territorial effect of UK GDPR

This will affect **EU/EEA** entities as well as non-EU/EEA entities. The UK government intends that the UK GDPR will have extra- territorial effect and also apply to controllers and processors based outside the UK if their processing relates to offering goods or services to individuals in the UK or monitoring the behaviour of individuals taking place in the UK.

EU/EEA/ UK representative review

Non-EU/EEA controllers who have appointed an EU/EEA representative in the UK for GDPR purposes will need to consider if they need to appoint a representative within the EU/EEA in addition or instead. After the UK has left the EU, businesses that do not have a presence in the EU or the UK but intend to offer goods and services and/or monitor individuals located in the UK and the EU/EEA may require both a UK representative under the UK GDPR and an EU/EEA representative under EU GDPR. EU/EEA entities bound by the UK GDPR will need to appoint a UK representative under the UK GDPR.

Penningtons Manches Cooper LLP is a limited liability partnership registered in England and Wales with registered number OC311575. It is authorised and regulated by the Solicitors Regulation Authority.

PENNINGTONS MANCHES COOPER

Identifying transfers so that compliance steps can be easily identified and implemented

For record-keeping purposes and to ensure that businesses are ready to implement the required compliance steps, multinational organisations should identify not only EU/EEA to non-EU/EEA transfers and personal data processing but also transfers to and from and processing activities within the UK.

Further guidance to help businesses prepare for the UK leaving the EU, including checklists and interactive tools, can be found on the ICO website **here**.

FIND OUT MORE

For further information, please contact:

JOANNE VENGADESAN
T: +44 (0)118 402 3833
E: joanne.vengadesan@penningtonslaw.com

DAN LOVETT
T: +44 (0)118 907 3486
E: dan.lovett@penningtonslaw.com

Penningtons Manches Cooper LLP is a limited liability partnership registered in England and Wales with registered number OC311575. It is authorised and regulated by the Solicitors Regulation Authority.