fox williams

BTA member webinar

Handling personal data – an overview

Please note that these slides are meant as general guidance only and should not be used as a substitute for legal advice.

Farina Azam
Partner

Agenda

- Legislation & Definitions;
- Key principles of GDPR;
- Legal conditions for processing personal data;
- Data subject's rights;
- International data transfers;
- Marketing in a B2B context.

Legislation

- The data protection legislation regime in the UK is set out in:
  - Data Protection Act 2018 (DPA 2018);
  - UK GDPR.
- From 1 January 2021, the EU GDPR no longer directly applies to the UK but it continues to be directly applicable in EU member states. It will also apply to UK businesses which operate in the EU or regularly offer travel services to customers in the EU.
- Data controller: The data controller determines how personal data is processed and the purposes for which it is processed. The data controller may use other companies to carry out processing services for them. In that case, the controller remains responsible for the processing of the data.
- Data processor: data processors are the entities processing the data on behalf of a data controller. Data protection legislation holds processors liable for breaches or non-compliance. It's possible that both the controller and processing partner will be liable for penalties even if the fault is entirely on the processing partner.
- A failure to comply with the provisions of the DPA/UK GDPR could attract a fine of up to 4% of annual worldwide turnover or 17.5 Million GBP whichever is greater.
- [Note: we're not going to dealing with data breaches, privacy notices or data subject access requests due to time constraints.]

Key principles of the UK GDPR

- The UK GDPR lays down several key principles which controllers and processors must comply with when processing personal data:
  - **Lawfulness, fairness and transparency.** Personal data must be processed lawfully, fairly and in a transparent manner in relation to the data subject. The controller must only process personal data on the basis of one or more of the following legal grounds set out in Article 6 of the UK GDPR
  - **Purpose limitation.** Personal data must only be collected for specified, explicit and legitimate purposes. It must not be further processed in any manner incompatible with those purposes
  - **Data minimisation.** Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.
  - **Accuracy.** Personal data must be accurate and, where necessary, kept up to date.
  - **Storage limitation.** Personal data must not be kept in a form which permits data subjects to be identified for longer than is necessary for the purposes for which the data is processed.
  - **Integrity and confidentiality.** Personal data must be processed in a way that appropriately ensures its security. Controllers and processors must use appropriate technical or organisational security measures to ensure this.
  - **Accountability.** The controller is responsible for, and must be able to demonstrate, compliance with the other data protection principles. Must also register with ICO.

Lawfulness of processing

A controller must only process personal data on one of the legal grounds set out in UK GDPR:

- Consent: you have obtained the consent for data processing from the person, or, if a child, their parent or guardian. (see next slide); or
- The processing is necessary for:
  - entering or the performance of a contract to which the data subject is party (e.g. contract which the person has entered into for a holiday or other arrangement or because they have asked for something to be done so they can enter into a contract);
  - compliance with a legal obligation to which the controller is subject (not an obligation under a contract);
  - protecting the vital interests of the data subject;
  - the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data is disclosed;
  - the purposes of the legitimate interests pursued by the controller or a third party except where those interests are overridden by the interests or fundamental rights and freedoms of the data subject. Must undertake a Legitimate Interest Assessment, and be able to show:
    - you need to process the information for the purposes of your legitimate interests or for those of a third party to whom you disclose it;
    - the processing is necessary for the purpose you have identified;
    - the impact on individuals' interests and rights and freedoms and assess whether this overrides your legitimate interests. The legitimate interests must be balanced against the interests of the individual(s) concerned.

Consent

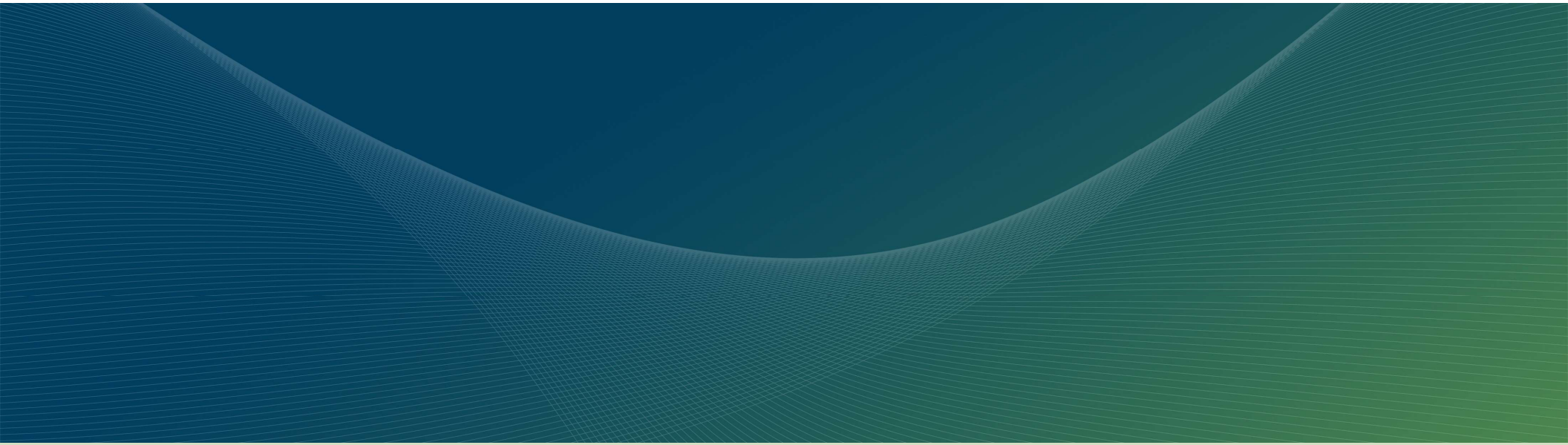
- The GDPR requires that consent be:
  - Freely given, specific, and informed.
  - Unambiguous and in the form of an affirmative action or statement.
  - Explicit for certain types of data processing, including, but not limited to, special category data processing and cross-border data transfers.
  - Presented in a manner clearly distinguishable from other matters in an intelligible and easily accessible form.
  - Provided in clear and plain language.
- Right to withdraw: Customers should have the opportunity to withdraw their consent at any time. You should make it easy for them to withdraw consent and publicise how to do so.
- Formal: You should be able at any time to prove that you have obtained consent from your customer. You should hold evidence of when, how, and what customers agreed to.

Data subject's rights

Data subjects have certain rights under the GDPR including the right to:

- Information: the right to be told that their data is being processed;
- Access to their own personal data;
- Correct personal data: to have personal data rectified if it is inaccurate or incomplete;
- Erase personal data*, also known as the right to be forgotten; or restrict data processing; or object to data processing: this could happen in the following circumstances:
  - the personal data is no longer necessary for the purpose which you originally collected or processed it for;
  - you are relying on consent as your lawful basis for holding the data, and the individual withdraws their consent;
  - you are relying on legitimate interests as your basis for processing, the individual objects to the processing of their data, and there is no overriding legitimate interest to continue this processing;
  - you are processing the personal data for direct marketing purposes and the individual objects to that processing;
  - you have processed the personal data without a proper legal basis;
  - you have to do it to comply with a legal obligation.
- Receive a copy of their personal data or transfer their personal data to another controller;
- Not be subject to automated decision-making;
- Be notified of a data security breach.
- *Note: the right to erasure doesn't apply where the processing is necessary to exercise the right of freedom of expression and information; to comply with a legal obligation; for the establishment, exercise or defence of legal claims.

International data transfers



International transfers of data (1)

The general principle is that personal data may only be transferred from the UK to a third country if one of the following conditions applies:

1. There's an adequacy decision in place for the third country whereby the third country has been deemed to provide an adequate level of protection for individuals' data protection rights following an assessment by the relevant govt body. Countries with an adequacy finding include the EEA & EFTA. (UK also has an adequacy finding from the EU).
2. There are appropriate safeguards in place:
    - Standard contractual clauses (SCC's) plus TRA:
        - EU SCC's: The Commission has issued standard contractual clauses for data transfers from data controllers in the EU to data controllers established outside the EU or EEA. It has also issued standard contractual clauses for data transfers from controllers in the EU to processors established outside the EU or EEA. Businesses can continue to use the Directive SCCs until they are no longer applicable for use under the UK GDPR on 21 March 2024, provided they were entered into on or before 21 September 2022.
        - UK SCC's: being the International Data Transfer Agreement (IDTA) and the Addendum prepared by the ICO and compliant with the UK GDPR. Came into force on 21 March 2022, and from 21 March 2024 will be the only sets of SCCs for facilitating restricted transfers under the UK GDPR.
        - Transfer Risk Assessment (TRA): The ECJ's decision in Schrems II specifically introduced the requirement that before a data exporter can rely on an Article 46 appropriate safeguard, it must conduct a TRA.
    - Binding corporate rules: If you transfer data internationally within a group company structure, you may use binding corporate rules to ensure the appropriate safeguards are in place. BCR arrangement will need to be approved by ICO.

International transfers of data (2)

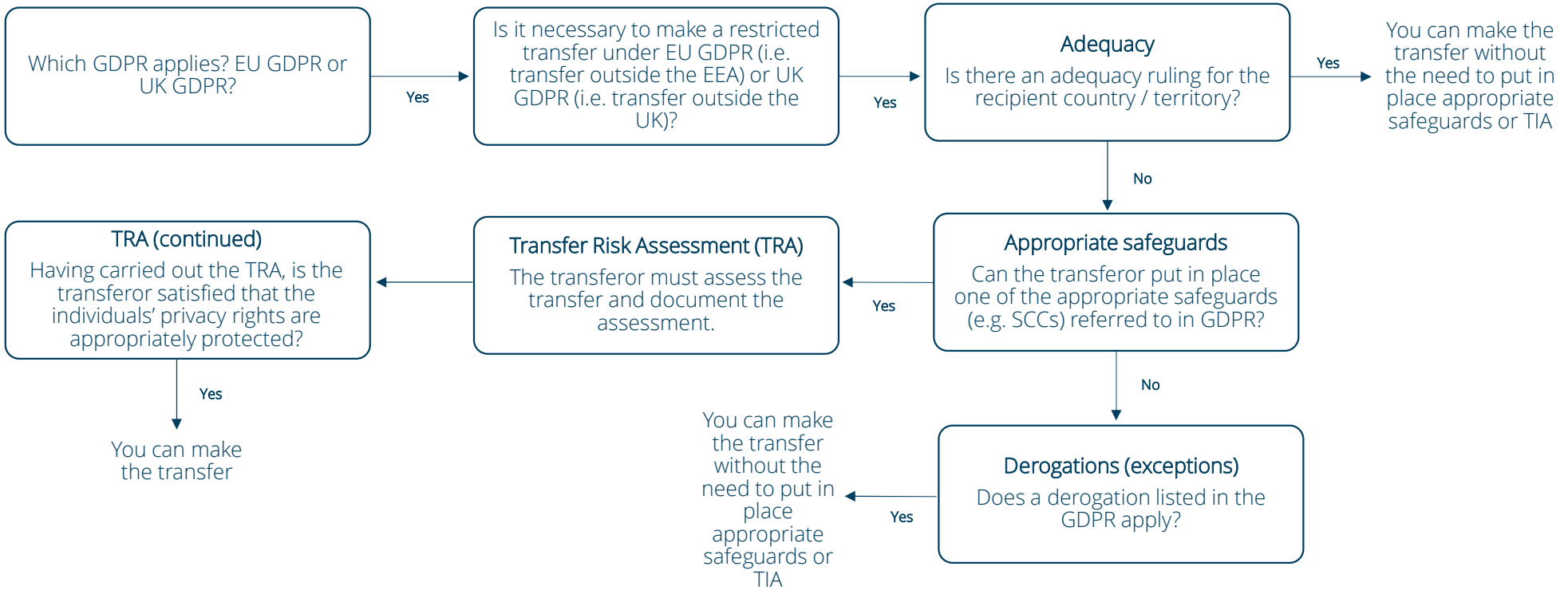
3. A specific "**exception"** (derogation) applies:

- Exception 1 - explicit consent: You may transfer data if you obtain the explicit consent of the customer, after you have informed them of the possible risks of such transfer due to the absence of adequacy regulations (or, under EU GDPR, adequacy decisions made by the Commission) and appropriate safeguards.
- Exception 2 - necessary for the performance of a contract between controller and data subject: If the transfer of data is occasional and not a regular process, you can transfer data on the basis that it is for the purpose of entering or for the performance of a contract.
- The ICO uses the following example: A UK travel company that offers bespoke travel arrangements may send personal data to a hotel in Peru, provided that it does not regularly arrange for its customers to stay at that hotel. If it did, it should consider using an appropriate safeguard such as the standard contractual clauses.
- Other exceptions are not relevant for the purposes of this training.

Adequacy and the new EU-US Data Privacy Framework

- List of (fully or partial) adequate territories (almost the same under EU & UK GDPRs):
  - Andorra, Argentina, Canada, European Economic Area, Faroe Islands, Guernsey, Isle of Man, Israel, Japan, Jersey, South Korea, Switzerland, United Kingdom, Uruguay, New Zealand
- In July 2023, the EU-US Data Privacy Framework was added to the above list
  - In October 2023, UK government implemented 'bridge' for UK Extension to DPF

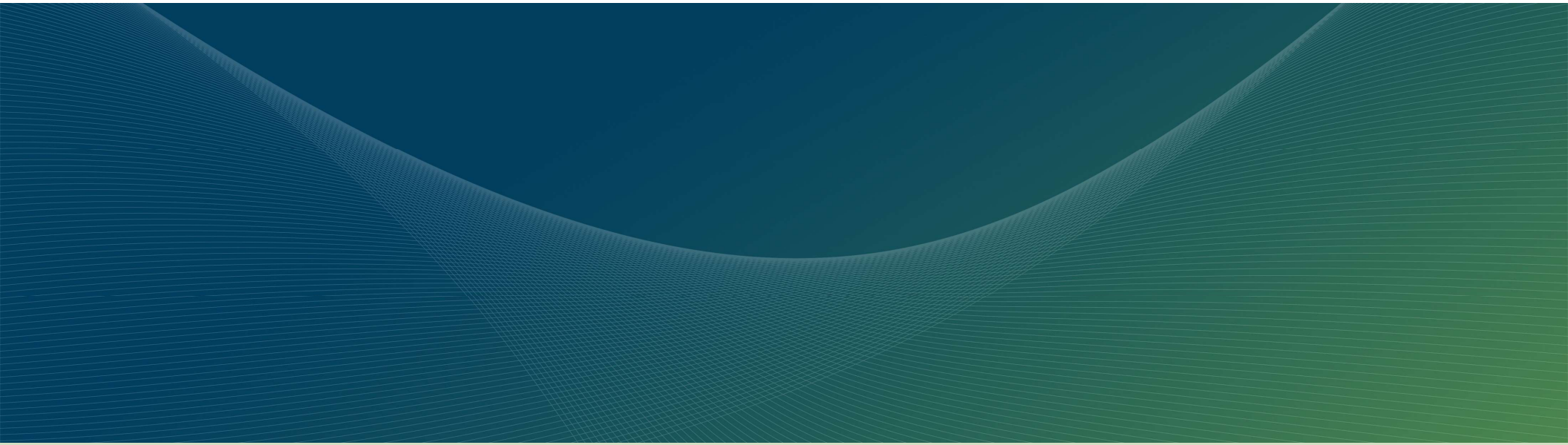
Summary of EU/UK laws on international data transfers (1)



Actions you should take

- Assess your international data flows / carry out data mapping
- Apply transfers to the applicable law
- Is your business subject to UK GDPR, EU GDPR, or both?
- Are you still relying on old EU SCCs? Prioritise making the transition to the new clauses
- Update data protection terms
- Put in place / update your intra-group data sharing agreement
- Carry out transfer risk assessment (when relying on SCCs)

Direct Marketing



Direct b2b marketing

- Direct marketing is where you want to promote your products and services and direct this to particular people.
- If, during your B2B marketing, you can identify individuals (directly or indirectly) then generally the UK GDPR and DPA 2018 apply.
- PECR also applies to B2B marketing – however rules are less strict
- Direct marketing can include:
  - emails;
  - text messages;
  - phone calls;
  - post;
  - social media marketing; or
  - targeted online adverts.
- It can also include background activities, such as profiling the people you want to send direct marketing messages to.

Direct marketing: lawful basis

- You must have a lawful basis for using people's information. For your direct marketing, the ones you're likely to use are consent or legitimate interests.
- Consent:
  - For consent to be valid, you must make it very clear to people exactly what they're consenting to, and they need to give their consent freely. This means you can't require consent in exchange for a service. You also need to make sure consent is given by an 'affirmative action' – or, in other words, the person actively takes a step to give you their consent. You can't use pre-ticked opt-in boxes. People can withdraw their consent at any time and you should make it as easy as possible for them.
  - If you're relying on consent, you can't use people's personal data for any purpose other than the one they originally consented to.
- Legitimate interest
  - You need to be able to justify that sending marketing is in your legitimate interests and you need to balance these interests against people's rights and expectations.

Direct marketing: telephone calls & post

- Before making live marketing phone calls, you must make sure you've checked your list against the Telephone Preference System (TPS) and your own 'don't contact' list. When you call, you must:
  - say who you are;
  - display your number; and
  - provide your contact details if asked.
- If you're making automated marketing calls, you must have consent from people that they're happy to receive these.

- If you're sending direct marketing to people by post, PECR marketing rules don't apply. But you still must comply with data protection law.

Direct marketing: emails

- PECR does not apply to electronic marketing to corporate subscribers, i.e. companies and LLPs, and government bodies.
- Therefore, you can email corporate subscribers without obtaining their consent.
- However, when sending direct marketing to people by email or text, you must give them a way to opt-out or unsubscribe.
- Under the PECR rules, sole traders and simple partnerships are classed as individuals under the rules. Therefore, you will need consent to email them unless they have purchased something from you before or used your services and didn't opt out of receiving marketing messages (known as 'the soft-opt in').

Questions?

Fox Williams: Travel Team

Rhys Griffiths
Partners
+44 (0)20 7614 2553
rgriffiths@foxwilliams.com

Lucy England
Partner
+44 (0)20 7614 2531
lengland@foxwilliams.com

Farina Azam
Partner
+44 (0) 207 614 2642
fazam@foxwilliams.com

Phyllis Acheampong
Senior Associate
+44 (0) 20 7614 2608
pacheampong@foxwilliams.com

Jessica Howard
Associate
+44 (0)20 7614 2647
jhoward@foxwilliams.com

Vladimir Arutyunyan
Associate
+44 (0)20 7614 2592
varutyunyan@foxwilliams.com