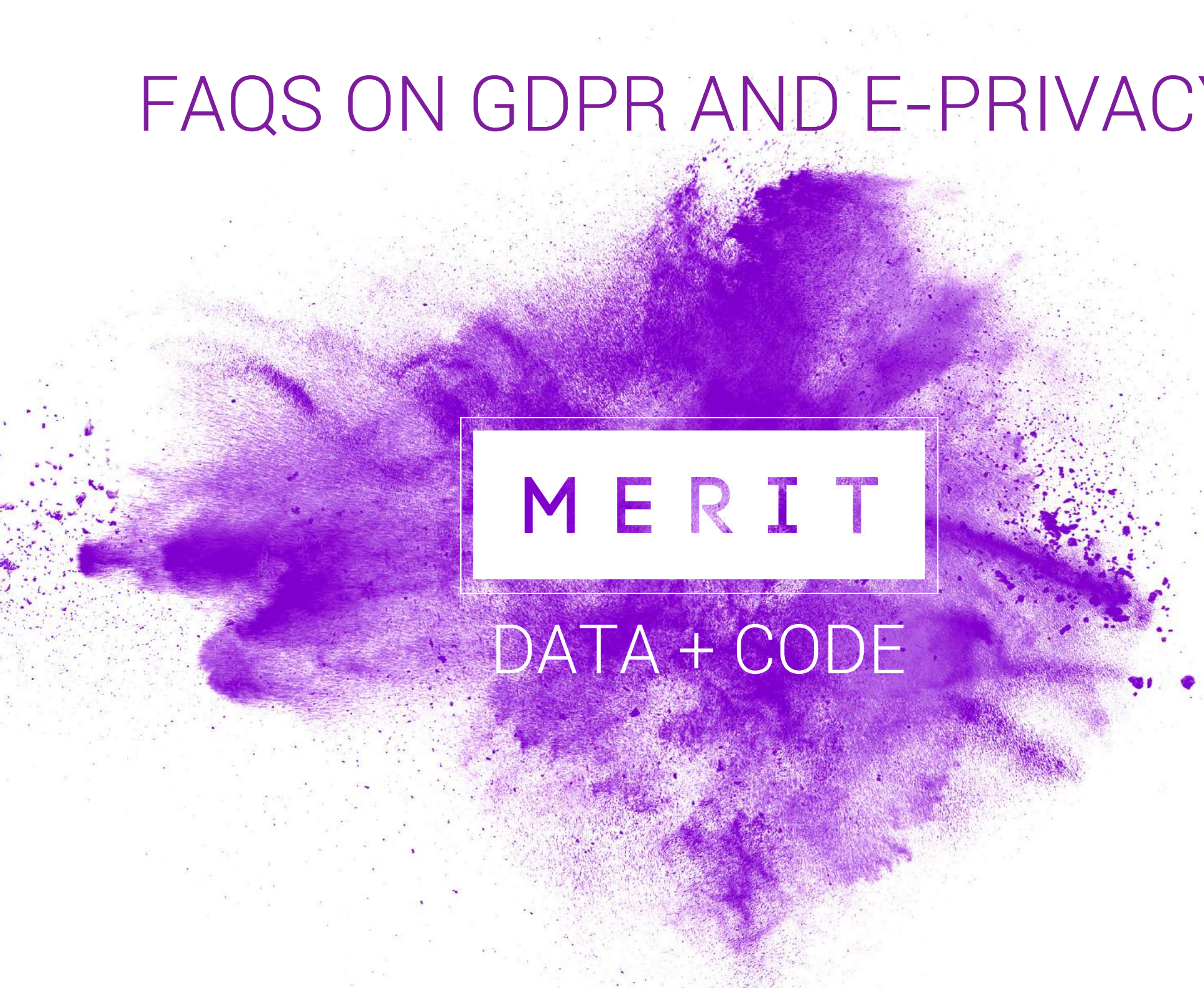
FAQS ON GDPR AND E-PRIVACY



CONTENTS

ABOUT

Merit is on a mission to ensure the successful evolution of the b2b information and media industry in the face of fundamental challenges and dramatic change - supporting brands to confidently embrace the future through DATA + CODE.

As forerunners on GDPR compliance (BS10012:2017), with a dedicated R&D team and the flexibility to react to changes quickly, Merit is prepared for future industry developments.

This FAQ addresses some of the most commonly asked questions in relation to GDPR, but if you have any further queries then please contact us at enquiries@meritgroup.co.uk

NEW DATA COLLECTION (1/2)

Can we collect/obtain new contact data for marketing purposes from the web? Or should we use old data held in our systems or database?

The statement on the right hand side of this page is based on Article 6 - Lawfulness of Processing of Regulation EU 2016/679 (GDPR):

'...(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks.'

In addition, Recitation 47 of the GDPR 2016/679/EU shows that processing of personal data (i.e. collection in this case) for direct marketing by the controller is clearly regarded as legitimate interest:

'...the processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest.'

By definition under Article 4 - Definitions of Regulation EU 2016/679 (GDPR), processing includes the collection or obtaining of personal data:

'Processing means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction'

Article 4 (2) - the definition of 'processing' includes collection, which can be by automated means or directly from the subject.

NEW PERSONAL DATA OR CONTACT DATA CAN BE COLLECTED BY ORGANISATIONS UNDER THE LEGITIMATE INTEREST CLAUSE OF THE GDPR

NEW DATA COLLECTION (2/2)

Can we only collect contact details directly from the data subject? Are we only able to use the contact details if they are voluntarily given by the data subject (e.g. when they visit a website)?

Not necessarily - the clauses/articles mentioned in the sections above support the collection and processing of personal data even if not obtained directly from the contact.

PERSONAL DATA CAN BE COLLECTED AND PROCESSED EVEN IF NOT OBTAINED DIRECTLY FROM THE CONTACT

GDPR ARTICLE REFERENCES

Article 6 Point 1.(f) of GDPR 2016/679 EU
Recitation 47 of GDPR 2016/679 EU
Article 4 Point 2 of GDPR 2016/679 EU

SUPPORTING LINKS

Guide to collecting and using personal information transparently:
https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-notices-transparency-and-control/

For more information visit: www.meritgroup.co.uk
Or contact us:
EMAIL: enquiries@meritgroup.co.uk
TEL: +44 845 226 0631

AUTOMATED ONLINE DATA GATHERING

Can robots or scraping programs be used to collect personal data from the web?

AUTOMATED MEANS CAN BE USED TO COLLECT DATA

The definition of the term 'processing' (see Article 4 of GDPR EU 2016/679) clearly shows that data can be collected by automated means.

At Merit, we use robots for personal data collection on some processes. However, when we do so we make sure that data collected is not used 'as is', and is further validated and augmented.

GDPR ARTICLE REFERENCES

Article 4 Point 2 of GDPR 2016/679 EU

For more information visit: www.meritgroup.co.uk
Or contact us:
EMAIL: enquiries@meritgroup.co.uk
TEL: +44 845 226 0631

CONSENT (1/4)

MERIT

Do we need consent from a data subject prior to sending out marketing communications?

CONSENT IS NOT A MUST FOR CONTACTING PEOPLE - ESPECIALLY FOR B2B CONTACTS

Consent is only one of six lawful bases of processing, with another being legitimate interest.

The GDPR clearly states that direct marketing can be considered a legitimate interest, thus allowing the processing of data without requirement of consent.

However, organisations are now worried about Privacy and Electronic Communication Regulations (PECR). This is the regulation that defines which types of marketing communication require prior opt-in and which ones do not.

Currently, every member state has its own PECR which is based on ePrivacy Directive 2002/58/EU. There are plans for this to be replaced with a EU-wide ePrivacy Regulation, which is currently in draft proposal stage.

Until the new ePrivacy regulation is announced, GDPR will be used in relation with the existing country-specific PECR regulation. This means that any marketing communications you were able to send on an opt-out or soft opt-in basis before May 2018, you will still be able to send on an opt-out basis when GDPR comes into force.

Take for example the UK, where the current PECR is based on the ePrivacy Directive 2002/58/EU and states that different, and usually less strict, rules apply to b2b communication - people within a legal entity may be contacted for direct marketing purposes, but certain safeguards should be taken (see 'Email Marketing under PECR').

The Direct Marketing Communication guide by ICO (based on PECR) clearly shows that consent is not applicable for B2B communication. However, the individual within the business has the right to opt-out of such communications. It is therefore important when sending emails that the recipient should be given an option to opt-out in line with the requirements of the PECR and GDPR.

GDPR ARTICLE REFERENCES
Article 6 Point 1.(f)
Recital 47 of GDPR 2016/679 EU

SUPPORTING LINKS
Lawful basis for processing - consent
https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/consent/

For more information visit: www.meritgroup.co.uk
Or contact us:
EMAIL: enquiries@meritgroup.co.uk
TEL: +44 845 226 0631

CONSENT (2/4)

Do we need to contact the data subject with an option to opt-out from further communications before sending out marketing communications?

Prior to marketing a product, event or service, it is good practice to inform the recipient or data subject of the details of the controller and why the person is being contacted, as well as provide an opt-in/out for future marketing communications.

However, this does not need to be sent as a separate email every time contact is made and can be combined with the actual marketing message.

Every email should include a link to a privacy notice that clearly states the details of the controller (a representative of the controller or the contact person) as well as any other relevant information that you need to supply to the individual under GDPR - see ICO guidance on the right of this page for a quick overview of what information should be provided in privacy notices under GDPR.

Providing this privacy notice at the time of the first marketing communication will then be in accordance with the following GDPR Articles:

Article 14 – "Information to be provided where personal data have not been obtained from the data subject"
Article 12 - "Transparent Information, communication and modalities for the exercise of the rights of the data subject rights" (Data subject rights are covered under Articles 15 through to Article 22)

PRIVACY NOTICES CAN BE INCLUDED WITH MARKETING COMMUNICATIONS AND DO NOT NEED TO BE SENT SEPARATELY

GDPR ARTICLE REFERENCES
Articles 12, 14, 15, 16, 17, 18, 19, 21 and 22 of the GDPR EU 2016/679

For more information visit: www.meritgroup.co.uk
Or contact us:
EMAIL: enquiries@meritgroup.co.uk
TEL: +44 845 226 0631

CONSENT (3/4)

MERIT

Can we continue sending marketing messages to a contact if they have not opted-out of receiving marketing communications? Is silence to be treated as consent?

Silence should not be treated as consent. Recitation 32 of the GDPR states the following:

"*Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement. This could include ticking a box when visiting an internet website, choosing technical settings for information society services or another statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of his or her personal data. Silence, pre-ticked boxes or inactivity should not therefore constitute consent. Consent should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent should be given for all of them. If the data subject's consent is to be given following a request by electronic means, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided.*"

However, if the marketing messages are being sent on the basis of legitimate interest, obtaining consent is not a pre-requisite to sending direct marketing messages. Refer to the relevant PECR on which types of electronic messaging require prior opt-in.

You must also ensure that you do not retain personal data for longer than necessary (see Data Retention section of this document).

LEGITIMATE INTERESTS CAN ALLOW THE SENDING OF COMMUNICATIONS WITHOUT PRIOR CONSENT

CONSENT (4/4)

MERIT

Can we use consent for receiving communications on one product or service to market other products or services by the organisation?

CONSENT ON NEW PRODUCTS/SERVICES CAN APPLY TO NEW PRODUCTS AND SERVICES IF THEY ARE SIMILAR TO THE ORIGINAL ITEM THAT GAINED CONSENT

GDPR does not explicitly discuss this point. However, Article 13: Unsolicited Communication of the Directive 2002/58/EU (which is the basis of the Privacy and Electronic Communication Regulations in the UK) states that the new product or service must be similar to the one that the customer originally purchased.

CONSENT - SUPPORTING LINKS

What are PECR?
https://ico.org.uk/for-organisations/guide-to-pecr/what-are-pecr/
Direct Marketing under PECR
https://ico.org.uk/for-organisations/guide-to-pecr/electronic-and-telephone-marketing/
The Conditions for Processing
https://ico.org.uk/for-organisations/guide-to-data-protection/conditions-for-processing/
Email Marketing under PECR
https://ico.org.uk/for-organisations/guide-to-pecr/electronic-and-telephone-marketing/electronic-mail-marketing/
Direct Marketing Guidance – page 38
https://ico.org.uk/media/for-organisations/documents/1555/direct-marketing-guidance.pdf
ICO Direct Marketing Checklist
https://ico.org.uk/media/for-organisations/documents/1551/direct-marketing-checklist.pdf
Conditions for Processing – Legitimate Interest
https://ico.org.uk/for-organisations/guide-to-data-protection/conditions-for-processing/
Blog clarifying the issue of consent in GDPR compliance
https://iconewsblog.org.uk/2017/08/16/consent-is-not-the-silver-bullet-for-gdpr-compliance/
10 things B2B marketers need to know about the GDPR and data protection
https://dma.org.uk/article/10-things-b2b-marketers-need-to-know-about-the-gdpr-and-data-protection
ICO – Marketing
https://ico.org.uk/for-organisations/marketing/
Direct Marketing under PECR (UK)
https://ico.org.uk/for-organisations/guide-to-pecr/electronic-and-telephone-marketing/
Right to be informed
https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-be-informed/

DATA RETENTION

How long should personal data be retained? Is there a standard duration or term for retaining personal data collected for a client?

There are no specific guidelines given in the GDPR or the ePrivacy Directive 2002/58/EU regarding data retention duration. Recitation 64 of the GDPR 2016/679 EU states that data should not be retained with the sole purpose of being able to react to potential requests.

The data protection principles on which GDPR is based clearly and emphatically state that it is important that data is not retained longer than is necessary.

DATA SHOULD NOT BE RETAINED FOR LONGER THAN IS NECESSARY

GDPR ARTICLE REFERENCES

Recitation 64 GDPR EU 2016/679

SUPPORTING LINKS

https://ico.org.uk/for-organisations/guide-to-data-protection/principle-5-retention/

For more information visit: www.meritgroup.co.uk
Or contact us:
EMAIL: enquiries@meritgroup.co.uk
TEL: +44 845 226 0631

DATA RE-USE

Can collected contact details continue to be used without being validated again?

Collected data cannot be re-used (if it is not reasonably recent) without validation. Merit's recommendation is that data that is more than one or two years old is not used without re-verification or validation.

MERIT'S RECOMMENDATION IS THAT DATA MORE THAN 1-2 YEARS OLD IS NOT USED WITHOUT RE-VERIFICATION

Article 5: 'Principles Relating to Processing of Personal Data' states that:

"*1. Personal data shall be:*
(a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');
(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');
(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');
(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');
(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');
(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality') "

GDPR ARTICLE REFERENCES
Article 5 of the GDPR 2016/679 EU

For more information visit: www.meritgroup.co.uk
Or contact us:
EMAIL: enquiries@meritgroup.co.uk
TEL: +44 845 226 0631

PECR/PRIVACY SHIELD

MERIT

What is the PECR/ePrivacy regulation? Does PECR override GDPR?

PECR stands for Privacy and Electronic Communication Regulations. Currently there is no standard EU PECR, with member states producing their own versions of the regulations (which by and large are similar to one another) based on ePrivacy Directive 2002/58/EU (which is referred to in GDPR).

However, in the context of GDPR enforcement, the EU is also looking at a common Digital Single Marketing Strategy which would enforce standardised PECR across all member states of the EU (including the UK).

A draft proposal of the PECR was released in January 2017: https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-privacy-and-electronic-communications

THERE IS CURRENTLY NO COMMON EU PECR, BUT STANDARDISED REGULATIONS ARE IN PROGRESS

PECR/PRIVACY SHIELD

What is Privacy Shield? Does this override GDPR on data transfers from the EU and Switzerland to the U.S.?

THE PRIVACY SHIELD FRAMEWORKS ALLOW U.S. COMPANIES TO TRANSFER PERSONAL DATA OF EU CITIZENS TO THE U.S.

The EU-U.S. and Swiss-U.S. Privacy Shield Frameworks were designed by the U.S. Department of Commerce, the European Commission and the Swiss Administration to provide companies on both sides of the Atlantic with a mechanism to comply with data protection requirements when transferring personal data from the European Union and Switzerland to the United States in support of transatlantic commerce.

The Privacy Shield program, which is administered by the International Trade Administration (ITA) within the U.S. Department of Commerce, enables U.S. based organisations to join one or both of the Privacy Shield Frameworks in order to be considered to have adequate level of protection to be authorised to transfer personal data of EU residents to the U.S. To join the Privacy Shield Framework, a U.S. based organisation is required to self-certify to the Department of Commerce and publicly commit to complying with the Framework's requirements.

SUPPORTING LINKS
https://iapp.org/news/a/we-read-privacy-shield-so-you-dont-have-to/

For more information visit: www.meritgroup.co.uk
Or contact us:
EMAIL: enquiries@meritgroup.co.uk
TEL: +44 845 226 0631

DATA BREACH

MERIT

In the case of a data breach where both the controller and the processor are outside of the EEA, which jurisdiction will apply?

This needs to be viewed on a case-by-case basis and will be decided by the legal authorities of the EU country where the case is tried or the complaint was originally made.

If either the controller or the processor are in the EEA, then the jurisdiction country is the country in which the Supervisory Authority to whom the complaint was made is located.

THE LEGAL AUTHORITIES OF THE COUNTRY WHERE THE CASE IS TRIED OR THE COMPLAINT WAS MADE WILL DECIDE WHERE JURISDICTION LIES

SUPPORTING LINKS
https://iapp.org/news/a/we-read-privacy-shield-so-you-dont-have-to/

For more information visit: www.meritgroup.co.uk
Or contact us:
EMAIL: enquiries@meritgroup.co.uk
TEL: +44 845 226 0631

DATA + CODE

If you have any questions about preparing for GDPR,
please contact Merit on enquiries@meritgroup.co.uk