Checklist

Records to be kept for GPR compliance

Type of record	Example of records to be retains by data controller
Records of processing activities, which are required to be maintained under Article (Art. 30)	• Name and details of your organisation (and where applicable, of other controllers, your representative and data protection officer). • Purposes of the processing. • Description of the categories of data subject and categories of personal data; • Categories of third party recipients of personal data. • Details of transfers to third countries including documentation of the transfer mechanism safeguards in place. • Storage periods for the different categories of data). • General description of technical and organisational security measures used.
Documentation to help demonstrate compliance with the obligation to assess risk and implement technical and organisational measures appropriate to the risk	• Policies and procedures for the incorporation of data protection mechanisms into the technical specification of IT systems and business practices. • Documentation showing consultation with any supervisory authority, documentation of data protection officer's advice. • Evidence of security measure testing and data privacy requirements for third parties that receive or access personal data. • Data protection impact assessments, audits and other risk assessments including: • *identification of risks, including high-risk data processing;* • *risk mitigation plans;* • *identification of the lawful basis for processing personal data;* • *verification that data processing complies with the regulation;* • *evidence of necessary safeguards in systems, networks and processing operations;* • *evidence of review of processing activities and risks in light of changes to programs, systems, or processes; and* • *confirmation that updates were made after program, system or process changes affecting data protection risk.*
Documentation to help demonstrate a lawful basis for processing personal data	• A record of the lawful basis and analysis used to determine this, • Policies and procedures (eg, for obtaining consent or regarding secondary use of personal data and how to determine whether use is compatible with the purpose and what to do if not), • A record of consents obtained. • Completed data protection impact assessments or other risk assessments.
Documentation to help demonstrate compliance with the privacy notice requirements	• Copies of any privacy notices provided. • Policies and procedures (e.g. when/how privacy notices are provided or on data subject rights).

Type of record	Example of records to be retains by data controller
Documentation to help demonstrate compliance with the GDPR's requirements for valid consent	• Copies of written and electronic consent forms • Policies and procedures (e.g. for obtaining consent (and parental consent), to respond to withdrawal of consent or to ensure that personal data is only used in accordance with the consent obtained).
Documentation to help demonstrate compliance with the requirements relating to processing sensitive personal data	• The grounds for processing sensitive personal data through data protection impact assessments or other mechanisms. • Policies and procedures on its collection and use and documentation to demonstrate valid privacy notices and consent.
Documentation to help demonstrate compliance with data subject rights	• Policies and procedures (e.g. for responses or on automated decision making). • Response letters/forms. • Evidence of a mechanism to update or correct data. • Inventory of requests, responses automated decision making and legal justification for processing. • Procedures to ensure data is used in accordance with any objections or restrictions.
Documentation to help demonstrate compliance with the GDPR's cross border transfer requirements	• Data inventory of processing activities identifying cross-border data transfers and the transfer mechanism relied on for each transfer; • Identification of any specific adequacy decision relied on to support the transfer. • Copies of valid consent forms relied on to support the transfer. • When relying on other derogations under Article 49 besides consent, identification of the specific transfer basis or a record of the assessment balancing the data controller's legitimate interests against the data subject's rights and freedoms. • When relying on other appropriate safeguards: • *documentation of compliance with the Privacy Shield;* • *approved binding corporate rules and related documentation;* • *data transfer agreements incorporating standard clauses;* • *documentation of compliance with an approved code of conduct or certification program; or* • *documented approval from the relevant supervisory authority.*
Documentation to help demonstrate compliance with Article 26 (Joint controllers)	• Details of the arrangement between joint controllers • A privacy notice that includes details on the joint controller relationship and a contact point for data subjects. • Policies and procedures on responding to data subject access or other requests.
Documentation to help demonstrate compliance with Article 28 (Processors)	• Policies and procedures e.g. for conducting DD on potential data processors, engaging data processors and executing contracts; • Completed DD reports or risk assessments; • Executed contracts that comply with Article 28 or include standard contractual clauses approved by European Commission or other supervisory authority. • Evidence of processor's adherence to an approved code of conduct referred to in Art 40

GDPR - getting data protection right

The EU General Data Protection Regulation (GDPR) and Data Protection Act 2018 are now in force. This has been described as “the biggest change to data protection law for a generation”. It’s not just us saying that – those are the words of the Information Commissioner, Elizabeth Denham.

There has been quite a lot of focus on the consequences of getting data protection compliance wrong, with headlines about fines of up to €20million, or 4% of global annual turnover if that is higher.

At Mills & Reeve we focus on the practical steps your organisation can take to get data protection compliance right

Get in touch

Richard Sykes
Partner
T +44(0)121 456 8436
richard.sykes@mills-reeve.com

Paul Knight
Partner
T +44(0)161 234 8702
paul.knight@mills-reeve.com

Peter Wainman
Partner
T +44(0)1223 222408
peter.wainman@mills-reeve.com

MILLS & REEVE
Achieve more. Together.

www.mills-reeve.com/GDPR