The EU General Data Protection Regulation

UK Steel
Broadway House
Tothill Street
London
SW1H 9NQ

The EU General Data Protection Regulation (GDPR) replaces the Data Protection Directive 95/46/EC and was designed to harmonize data privacy laws across Europe, to protect and empower all EU citizens' data privacy and to reshape the way organizations across the region approach data privacy. Enforcement date: 25 May 2018 - at which time those organizations in non-compliance will face heavy fines. This note sets out an overview of UK Steel's interpretation of the General Data Protection Regulation (GDPR).

GDPR planning and preparation. If you process data about individuals in the context of selling goods or services to citizens in other EU countries then you will need to comply with the GDPR, irrespective as to whether or not you the UK retains the GDPR post-Brexit. If your activities are limited to the UK, then the position (after the initial exit period) is less clear. The UK Government has indicated it will implement an equivalent or alternative legal mechanisms. However, this is likely to follow the GDPR.

Who does the GDPR affect? The GDPR not only applies to organisations located within the EU. It will also apply to organisations outside of the EU if they offer goods or services to, or monitor the behaviour of, EU data subjects. It applies to all companies processing and holding the personal data of data subjects residing in the European Union, regardless of the company's location.

Penalties for non-compliance? Organizations can be fined up to 4% of annual global turnover for breaching GDPR or €20 Million. There is a tiered approach to fines e.g. a company can be fined 2% for not having their records in order (article 28. It is important to note that these rules apply to both controllers and processors -- meaning 'clouds' will not be exempt from GDPR enforcement.

What constitutes personal data? Any information related to a natural person or 'Data Subject', that can be used to directly or indirectly identify the person. It can be anything from a name, a photo, an email address, bank details, posts on social networking websites, medical information, or a computer IP address.

What is the difference between a data processor and a data controller? A controller is the entity that determines the purposes, conditions and means of the processing of personal data, while the processor is an entity which processes personal data on behalf of the controller.

Do data processors need 'explicit' or 'unambiguous' data subject consent? The conditions for consent have been strengthened, as companies will no longer be able to utilise long illegible terms and conditions full of legalese. The request for consent must be given in an intelligible and easily accessible form, with the purpose for data processing attached to that consent - meaning it must be unambiguous. Consent must be clear and distinguishable from other matters and provided in an intelligible and easily accessible form, using clear and plain language. It must be as easy to withdraw consent as it is to give it. Explicit consent is required only for processing sensitive personal data - in this context, nothing short of "opt in" will suffice.

Does my business need to appoint a Data Protection Officer (DPO)? DPOs must be appointed in the case of: (a) public authorities, (b) organizations that engage in large scale systematic monitoring, or (c) organizations that engage in large scale processing of sensitive personal data. If you are not in one of these categories, then you do not need to appoint a DPO.

How does the GDPR affect policy surrounding data breaches? Proposed regulations surrounding data breaches primarily relate to the notification policies of companies that have been breached. Data breaches which may pose a risk to individuals must be notified to the DPA within 72 hours and to affected individuals without undue delay.

Processing lawfully - the data protection principles. As well as imposing certain specific obligations the GDPR requires you to process data in compliance with various data protection principles. You need to

comply with all of these principles to be sure that you are processing personal data lawfully. We summarise them below.

Principle	What it means
Fair, lawful and transparent processing	You must: • tell employees what information you hold about them and what you do with it (the GDPR concept of 'granularity' means this information must be quite detailed) • handle employees' information only in ways they would reasonably expect • not use personal data in a way that has an *unjustified* adverse impact on the employee (it can have an adverse impact, as long as it is justified) • Ensure that you have a 'legal basis' for processing their ordinary personal data (see below) • if you are processing special category data, ensure that you *also* have a 'special category' legal basis for doing so (see below)
Obtain personal data for specified, explicit and legitimate purposes and do not process it in a way which is incompatible with those purposes	You need to tell employees the purposes for which you need their information and avoid using it for different reasons. If you need to use information for a different purpose, you must take into account the following factors when deciding if the new purpose is compatible with the original purpose: • Is there a link between the new and old purpose? • Context of data collection and the relationship between the parties • Nature of the data – e.g. is it special category data? • Consequences of processing • What safeguards are in place?
Personal data must be adequate, relevant and limited to what is necessary for the purposes for which it is processed	Do not obtain or hold excessive, disproportionate or irrelevant amounts of data about employees. This is part of a principle referred to as 'data minimisation'.
Data must be accurate	Keep information you hold about employees accurate and up-to-date.
Do not keep data for longer than necessary for the purposes for which it is processed	Do not retain personal data for any longer than you need in order to meet the purpose for which it is held. This is part of a principle referred to as 'data minimisation'. You can find guidance on retention periods in Retention and deletion of HR records.
Keep information secure	Ensure that employee's information is kept secure and confidential. Take steps to make sure it is not lost, destroyed or damaged and is available to people only on a need to know basis.
Demonstrate compliance with the principles	The GDPR introduces a new concept of 'demonstrable compliance' or the 'accountability principle' which means that it is not enough for you to comply with each of the principles set out above; you must also be able to *demonstrate* that you do.