INCLUSIVE SKATING

Advice note on GDPR accountability

What is the accountability principle?

The accountability principle in Article 5(2) requires you to demonstrate that you comply with the principles under the General Data Protection Act (**GDPR**) and states explicitly that this is your responsibility as a data controller. It is therefore not enough to be compliant with the GDPR, but you must also now be able to demonstrate your compliance.

In addition to Article 5(2), Article 24(1) of the GDPR also requires data controllers to demonstrate that their data processing activities comply with the GDPR's requirements. Together, Articles 5 and 24 form the concept of accountability under the GDPR.

Meeting the accountability requirement means doing more than just establishing data protection policies and procedures. Accountability requires you to be able to demonstrate compliance with the GDPR by showing the supervisory authority and individuals concerned how you are complying, on an ongoing basis, through evidence of:

- Internal policies and processes that comply with the GDPR's requirements;
- The implementation of the policies and processes into the organisation's activities;
- Effective internal compliance measures; and
- External controls.

The obligation to demonstrate compliance replaces the obligation to notify local data protection authorities such as the ICO of your processing activities ***(i.e. you will no longer have to register as a data controller with the ICO, but please note that annual fees will still be payable).***

What does this mean in practical terms?

The GDPR imposes many different obligations that require the data controller or data processor to demonstrate compliance with the GDPR's requirements. This means that, going forward, your organisation should be:

- establishing and maintaining a comprehensive data protection compliance program and appointing individuals responsible for overall data protection matters as part of the program, such as, where appropriate, a data protection officer (see ***Advice Note on Data Protection Officer appointment***). For example, this will mean assigning responsibility for implementing and maintaining a privacy compliance program, educating senior management about the GDPR's requirements and the impact of non-compliance, identifying key stakeholders (e.g. HR managers, finance managers, your managing director, those in sales, performance, etc.) and establishing reporting lines and regular communication between those appointed to oversee data protection compliance and your internal stakeholders;
- implementing appropriate technical and organisational measures that ensure and demonstrate that you are complying. This may include internal data protection policies such as staff training, internal audits of processing activities, and reviews of internal HR policies as well as evidence of regular security measure testing and an evaluation of those measures' effectiveness. When assessing the appropriate level of security that needs to be applied to the processing, you should consider the risks presented by processing the personal data, including the risks associated with accidental or unlawful destruction, loss, alteration, unauthorised disclosure, or access to personal data;
- implementing measures that meet the principles of data protection by design and data protection by default. The GDPR requires data controllers to integrate data protection into the design of their systems to ensure the inclusion of appropriate technical and organisational GDPR compliance measures into personal data processing. They must also implement "privacy by default" measures to ensure that, by default, they only process the personal data necessary for each specific purpose. Measures could include for example:
    - minimising the amount and categories of personal data you process;
    - anonymizing or pseudonymizing certain data;
    - incorporating transparency into all your data processing activities;
    - allowing individuals to monitor processing; and
    - creating and improving security features on an ongoing basis.
- *using data protection impact assessments (DPIA) where appropriate* - Article 35 GDPR introduces a formal requirement for organisations, in their role as data controllers, to conduct a DPIA before undertaking any processing that presents a specific privacy risk i.e. *"Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing is likely to result in a high risk to the rights and freedoms of natural persons."* The GDPR does not formally define what must be covered by a DPIA, but Article 35(7) sets out the following minimum requirements:
    - A systematic description of the proposed processing operations.
    - The purposes of the processing.
    - The legitimate interest pursued by the controller.
    - An assessment of the necessity and proportionality of the processing operations in relation to the purposes.

- An assessment of the risks to the rights and freedoms of data subjects.
- The measures envisaged to address the risks, including appropriate:
    - safeguards;
    - security measures; and
    - mechanisms to ensure the protection of personal data and to demonstrate compliance taking into account the rights and legitimate interests of data subjects and other persons concerned.

(see Inclusive Skating GDPR Compliance Questionnaire for further information on when to carry out a further data protection impact assessment and for the responses to the current questionnaire);

- complying with processing obligations and documenting compliance including:
    - determining and documenting a lawful basis for each instance of processing personal data and maintaining a record of data processing activities i.e. by keeping a written record of:
        - the name and contact details of the data controller, any representative of the data controller and the data protection officer if applicable);
        - the purposes of data processing.
        - a description of the categories of data subjects and categories of personal data.
        - the categories of third-party data recipients including recipients in other countries.
        - for transfers to other countries, identification of the country and the safeguards used to secure the transfer.
        - storage periods for the different categories of personal data.
        - a general description of the technical and organizational security measures used to secure the personal data.

        (NB: If your organisation has 250 or more employees, you must document all your processing activities. If your organisation has fewer than 250 employees, you only need to document processing activities that are (i) not occasional; (ii) result in a risk to the rights and freedoms of individuals; or (iii) involve the processing of special categories of data or criminal conviction and offence data. This means this exemption will often not apply.)
    - providing data subjects with GDPR-compliant privacy notices ***(see Privacy Notice templates)***;
    - satisfying specific requirements when relying on data subject consent ***(see drafting notes to Privacy Notice templates)***;
    - satisfying specific requirements when processing sensitive personal data ***(see drafting notes to Privacy Notice templates)***;
    - honouring data subject rights ***(see Guide to Data Subjects Rights, including Subject Access Requests and Right to be Forgotten)***; and

- complying with cross-border data transfer restrictions and maintaining compliant data transfer mechanisms ***(see Advice Note on Data Transfers Outside of the EEA)***.

- Delivering ongoing data protection training to staff. One of a data protection officer's responsibilities is to advise employees of their obligations under the GDPR and other applicable data protection laws, including providing training to employees involved in personal data processing. Training is not an explicit GDPR obligation for organisations that are not required to appoint a data protection officer. However, to embed data protection into the organisation's operations and daily activities effectively it should still implement regular data protection training;

- Implementing documentation to help demonstrate compliance with the GDPR's personal data breach notification requirements e.g. to do this, your organisation may (i) develop a security breach response plan including a protocol for notifying regulators, law enforcement, other agencies, and data subjects,(ii) nominate a security breach response team; and (iii) develop a log for recording security incidents and security breaches, including a summary of the incident, its effects, and the responsive action taken ***(see Advice note on Data breaches and self-reporting);***

- Taking certain steps when engaging data processors and managing third-party relationships ***(see data processing agreements templates).***

Why does our organisation need to comply with the Accountability principle?

Failure to comply with the accountability principle may result in fines of up to EUR20 million or 4% of the organisation's total worldwide annual revenue for the preceding financial year, whichever is higher.

A data controller or data processor's ability to present evidence to regulators of its efforts to comply with the requirements of the GDPR however may help reduce liability under GDPR. For example if your organisation can demonstrate, for example, that it did not act intentionally in violating the GDPR and that it implemented technical and organisational measures appropriate to the risk, a supervisory authority may consider this in deciding whether to impose a fine or it may reduce the fine imposed. In addition, *Article 82(3)* states that a data controller or data processor is exempt from liability if it proves that it was not responsible for the event resulting in damage.

Beyond GDPR compliance, the measures you implement around the accountability principle will help your organisation make the most of how it processes personal data, become more efficient and gain a reputation for being an organisation that people can trust to protect their personal data.

For more detailed guidance on your Accountability obligations under the GDPR, please see https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance