GOOD PRACTICE FOR DATA PROTECTION COMPLIANCE

In July 2023, the UK's Information Commissioner's Office (ICO) published three lessons to be learned from the reprimands that it issued in Q1 (April-June 2023).[1] The ICO expects the targeted organisations to improve their practices as set out in its reprimands, and also expects other organisations to learn from such enforcement actions so as to handle personal data appropriately.

1 ICO. (2023). *Lessons learned from reprimands.* Available at: Lessons learned from reprimands | ICO

This briefing sets out the three lessons to be learned from the ICO's Q1 reprimands, and lists "dos" and "don'ts" for organisations to follow to ensure that they remain compliant. This briefing also includes some general tips for compliance with data protection law, both in the UK and the European Economic Area.

The ICO's Lessons

Lesson 1: Implement policies and training to prevent inappropriate disclosure of personal data

Organisations should ensure that all data protection policies, procedures and guidance are thorough and include how to detect and report a personal data breach.

- **Don't** enable the inappropriate disclosure of personal information.
- **Do** implement policies regarding the displaying of personal information on electronic screens.
- **Do** provide adequate training for staff to redact and dispose of documents correctly.
- **Do** ensure that appropriate organisational and technical procedures are established to protect the security and confidentiality of internal emails, especially those containing sensitive or special category personal data.

Lesson 2: Respond to information access requests in a timely manner

In Q1, organisations were reprimanded for not responding to Subject Access Requests (SARs) within the statutory timeframe.

Individuals have the right to ask organisations for a copy of and information on their personal data, including where the information has been taken from, what it is being used for, and who it is being shared with.

When an organisation receives an SAR, it must respond within one month of receipt of the request. An extension of two months may apply if the SAR is complex.

- **Do** respond to SARs within the relevant time period.
- **Do** take a proactive approach to dealing with SARs.

Lesson 3: Take a 'by design and default' approach to data protection

Data protection by design and default is a legal requirement of the GDPR. It means putting in place *"appropriate technical and organisational measures to implement the data protection principles effectively and safeguard individual rights"*.[2] Data protection is integrated into processing activities and business practices from the beginning of the design stage. This means that data protection should be considered at the same time as business design, ensuring compliance and accountability with regards to the GDPR's fundamental principles and requirements.

This principle extends to an organisation's development and deployment of any new apps or software.

- **Do** consider the method and means of data processing before an app is deployed to ensure processing is compliant with data protection law.
- **Do** issue data protection guidance to staff regarding the use of any apps and require staff to confirm that issued guidance has been read and understood.

General tips for compliance with data protection law in the UK and European Economic Area

The UK and EU GDPR set out seven key principles which should inform an organisation's approach to processing personal data. The seven principles are:

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality (security)
- Accountability

The following are some general tips for compliance with data protection law in the UK and European Economic Area based on the seven principles.[3/4]

1. Provide individuals with privacy information. This is the information which your organisation must provide to individuals when collecting their personal data. Privacy information includes your organisation's purpose(s) for processing the individual's personal data, data retention periods, and who the data will be shared with.[5] Providing privacy information will enable your organisation to comply with the individual's right to be informed.
2. Keep accurate records of your organisation's purpose(s) for processing personal data, the source(s) of personal data, steps taken by your organisation to comply with GDPR and, where relevant, processing activities undertaken by your organisation. Records of processing activities (ROPA) are only required by organisations that employ more than 250 people, unless the processing *"is likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes special categories"* of personal data.[6] When the Data Protection and Digital Information (No. 2) Bill currently being considered by Parliament is enacted in the UK and enters into force, under UK law a ROPA will only be required by organisations whose processing *"is likely to result in a high risk to the rights and freedoms of individuals"*.[7]
3. Regularly review the personal data that your organisation holds. Erase or anonymise any data which your organisation no longer requires.

2 ICO. (2023). *Data protection by design and default.* Available at: Data protection by design and default | ICO

3 ICO. (2023). *A guide to the data protection principles.* Available at: A guide to the data protection principles | ICO

4 ICO. (2023). *Guide to accountability and governance.* Available at: Guide to accountability and governance | ICO

5 ICO. (2023). *A guide to individual rights: Right to be informed.* Available at: A guide to individual rights | ICO

6 Article 30 GDPR

7 Data Protection and Digital Information (No. 2) Bill

4. Establish and implement an information security policy, and maintain strong security measures. The policy should:
   - ensure that only required employees have access to personal data;
   - set out when encryption and/or pseudonymisation are appropriate; and
   - specify your organisation's backup processes.
5. Regularly review and (where necessary) update your organisation's privacy information, and data protection, data retention, data breach and information security policies.
6. Provide training to staff on the organisation's data protection, data retention, data breach and information security policies and procedures.
7. If your organisation uses third parties to process personal data, such arrangements should be set out in written contracts.
8. Carry out a Data Protection Impact Assessment (DPIA) when your organisation carries out a new form of data processing or the scope of existing data processing increases, and such processing is likely to result in high risk to individuals' interests.
9. Appoint a Data Protection Officer (DPO) where required or an alternative person to manage the organisation's compliance with data protection law.

For further information, please contact.

ANTHONY WOOLICH
Partner, London,
T +44 (0)20 7264 8033
E anthony.woolich@hfw.com

Assistance provided by Ruth Stillabower, Trainee Solicitor, London.

HFW has over 600 lawyers working in offices across the Americas, Europe, the Middle East and Asia Pacific. For further information about our EU, Competition and Regulatory capabilities, please visit hfw.com/EU-Competition-and-Regulatory.