GDPR

Emma Loveday-Hill
Associate
elovedayhill@prettys.co.uk
01473 298266

Agenda

- Introduction
- Data protection – the basics
- What data do you hold – audit exercise
- Audit results – what to do next
- Using data properly – minimising the risk of liability
- Embedding compliance – systems and policies
- Conclusions and questions

Prettys

Introduction

- Old law is Data Protection Act 1998
- General Data Protection Regulations
- Data Protection Bill

Prettys

Data Protection – the basics

Personal Data – "Any information relating to an identified or identifiable natural person ("**data subject**"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person"

Prettys

Data protection – the basics

Processing – "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"

Prettys

Data protection – the basics

Controller – "the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data"

Prettys

Data protection – the basics

Processor – "the natural of legal person, public authority, agency or other body which processes personal data on behalf of the controller"

Data protection – the basics

The Principles

"Personal data shall be:

(a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('**lawfulness fairness and transparency**')**[the First Principle]**;

(b) collected for specific, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes ('**purpose limitation**')**[the Second Principle]**;

Prettys

Data protection – the basics

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('**data minimisation**')**[the Third Principle]**;

(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**')**[the Fourth Principle]**

Prettys

Data Protection – the basics

(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 ('**storage limitation**')**[the Fifth Principle]**;

(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**')**[the Sixth Principle]**

Prettys

Data Protection – the basics

The Accountability Principle:

"The controller shall be responsible for, and able to demonstrate compliance with, the [Principles]"

Prettys

Data Protection – the basics

Special categories of personal data

"Processing of data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purposes of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation **shall be prohibited…**"

Prettys

Data Protection – the basics

…unless

- The data subject has given explicit consent;
- Processing is necessary for the purposes of specific rights and obligations of the data subject/data controller in respect of employment, social security or social protection law;
- Processing is necessary to protect the vital interests of the data subject;
- Processing is conducted by a not-for-profit body with a political, philosophical, religious or trade union aim insofar as the processing relates solely to its members;
- The data subject has already made the data public;
- Processing is necessary for the establishment, exercise or defence of legal claims ;

Prettys

Data Protection – the basics

(Continued)

- Processing is necessary for reasons of substantial public interest;
- Processing is necessary for the purposes of preventative or occupational medicine, for the assessment of working capacity of the employee, medical diagnosis, the provision of health or social care or treatment, or the management of health or social care systems and services;
- Processing is necessary for reasons of public interest in the area of public health;
- Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes.

Prettys

Data Protection – the basics

Transfers of personal data to third countries (ie outside of the European Economic Area)

Transfers should only take place if:

- There is an adequacy decision with regards to that country; or
- The data subject has explicitly consented to the transfer; or
- The transfer is necessary for the performance of a contract between or in the interests of the data subject or controller;
- The transfer is necessary for important reasons in the public interest;
- Other appropriate safeguards are in place, in particular:
    - Binding corporate rules;
    - The parties are subject to an agreement containing standard data protection clauses; or
    - There is an approved code of conduct applying backed up with binding and enforceable commitments.

Prettys

The audit – What data do you hold and what do you do with it?

Questions to Ask

- What personal details about individuals do I keep in my department?
- How are these details obtained?
- How are these details stored?
- How are these details used?
- Are these details deleted as soon as I have no more need for them?
- Do the people whose information I hold know that I've got it?
- Do I set out why these details are being used to the individual?
- Who do I disclose these details to internally?
- Why do I disclose these details internally?
- Who do I disclose these details to externally
- Why do I disclose these details externally?

Prettys

Using the audit results

- Am I processing data lawfully?
- Written record of processing activity
- Privacy information notices

Prettys

Using the audit results – lawful processing

Am I processing data lawfully?

a. Consent

b. Necessary for the performance of a contract with the data subject

c. Necessary for compliance with a legal obligation by the controller

d. Necessary in order to protect the vital interests of the individual or of another person

e. Necessary for the performance of a public interest task or in exercising an official authority vested

f. Necessary for the purposes of the legitimate interests pursued by the data controller

Prettys

Using the audit results – lawful processing

Consent

Valid consent only if:

- Positive, affirmative action
- Specific and unambiguous
- Freely given (e.g. performance of a contract cannot be conditional on this)
- Signifies the individual's agreement to their personal data being processed.
- Separate and distinguishable (e.g. separate form)
- Clearly presented
- Revocable

Prettys

Using the audit results – record keeping

Record keeping – what to document

- The name and contact details of your organisation (and where applicable, of other controllers, your representative and your data protection officer).
- The purposes of your processing.
- A description of the categories of individuals and categories of personal data.
- The categories of recipients of personal data.
- Details of your transfers to third countries including documenting the transfer mechanism safeguards in place.
- Retention schedules.
- A description of your technical and organisational security measures.

Prettys

Using the audit results - transparency

Privacy Information Notices

When to issue?

- If the data is obtained from the subject: at the time the data are obtained.
- If the data is obtained from elsewhere:
    - Within a reasonable period of having obtained the data (within one month)
    - If the data are used to communicate with the individual, at the latest, when the first communication takes place; or
    - If disclosure to another recipient is envisaged, at the latest, before the data are disclosed.

Prettys

Using the audit results - transparency

- Who will need a privacy information notice and when?
- In what format will you need to deliver this notice?
- What will be in the notice?

Prettys

Enforcement

- Fines
- Data breach reporting/notification process
- Powers of the ICO
- Civil claims

Prettys

Enforcement - Fines

A. Up to **2% of annual worldwide turnover** of the preceding financial year or **10 million euros** (whichever is the greater) for violations relating to internal record keeping, data processor contracts, data security and breach notification, data protection officers, and data protection by design and default

B. Up to **4% of annual worldwide turnover** of the preceding financial year or **20 million euros** (whichever is the greater) for violations relating to breaches of the data protection principles, conditions for consent, data subjects rights and international data transfers

Prettys

Enforcement - Data breaches

What is a personal data breach?

"A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data…

A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable and this unavailability has a significant negative effect on individuals…

When a personal data breach has occurred, you need to establish the likelihood and severity of the resulting risk to people's rights and freedoms. If it's likely that there will be a risk then you must notify the ICO; if it's unlikely then you don't have to report it. However, if you decide you don't need to report the breach, you need to be able to justify this decision, so you should document it." (Information Commissioners Office, 2017)

Prettys

Enforcement - Data breaches

Personal data breaches can include:

- access by an unauthorised third party;
- deliberate or accidental action (or inaction) by a controller or processor;
- sending personal data to an incorrect recipient;
- computing devices containing personal data being lost or stolen;
- alteration of personal data without permission; and
- loss of availability of personal data.

Prettys

Enforcement – data breaches

Information to include in the breach notification:

1. Categories and approximate number of individuals concerned;
2. Categories and approximate number of personal data records concerned;
3. Name and contact details of the DPO or other contact point where more information can be obtained;
4. Description of likely consequences;
5. Description of measures taken/ proposed to deal with the breach and (where appropriate, of the measures taken to mitigate any possible adverse effects).

Prettys

Enforcement - Data breaches

How do we minimise data breaches?

- Appropriate Security Measures
- Training
- Familiarisation/education
- Sanctions for breach

Prettys

Enforcement – Powers of the ICO

- Remains the independent regulator of personal data use in the United Kingdom
- Focus remains ensuring compliance through guidance and recommendations as to best practice
- Will continue to deal with complaints from individual data subjects
- Increased powers to enter premises, investigate and inspect
- Increased ability to sanction, and order compliance.

Prettys

Enforcement – Civil claims

- Individuals will have increased rights
- Complaints to ICO will remain the primary recourse for individuals
- Increased rights means a likelihood of increased claims
- Currently compensation for breach is low; that is likely to change
- More class actions

Prettys

Enforcement - individual rights

The right to…

- Be informed
- To rectification and erasure
- Access to data (Subject Access Requests)
- Data portability
- To restrict processing
- To be forgotten
- Object to processing

Prettys

Enforcement – individual rights

Subject Access Requests

- **Fees** prohibited (standard £10 no longer allowed) unless excessive or manifestly unfounded
- Tighter timeframes- without delay and at the latest within **1 month** of receipt
- Endeavour to have a system in place that provides for individual access to personal data (e.g. a central portal)
- The **identity** of the person needs to be verified first using "reasonable means".
- If the request is received electronically, the response should also be electronic.

Prettys

Enforcement – Individual rights

Data portability

- Individuals can obtain and reuse their personal data from data controllers to use for their own purposes in a **compatible format**
- Individuals can request the direct **transmission** from one data controller to another.

Prettys

Enforcement – Individual rights

The right to be forgotten

When can a request for erasure of data be made?

- Processing is no longer necessary to fulfil the original processing purpose
- Consent has been withdrawn
- Objection to processing/no legitimate interest
- Unlawfully processed
- Compliance with a legal obligation

Prettys

Enforcement – Individual rights

Right to restrict processing

- Automated decision making
- Profiling

Prettys

Embedding Compliance – systems and policies

Responsibility for compliance

- Do we need a Data Protection Officer (DPO)?
- If not, how will we manage data protection?

Prettys

Embedding compliance – systems and policies

Information security – Cyber Essentials

- Boundary firewalls and internal gateways
- Secure configuration
  - Remove unused software and services
  - Change default passwords
- Access control
  - User names and passwords
  - Appropriate individual permissions
- Malware protections
  - Up-to-date anti-virus and anti-malware products
- Patch management and software updates

Prettys

Embedding compliance – systems and policies

Checklist

- Data protection on the move
- Physical security
- Encryption
- Bring your own device (BYOD) policy
- Cloud storage
- Back ups
- Staff training
- Vulnerability scans and penetration tests

Prettys

Embedding compliance – systems and policies

Relationships with others

To who do we provide data?

- Who are our data processors?
- Do we have written contracts that govern the following:
    - Subject matter and duration of processing
    - only act on the written instructions of the controller;
    - ensure that people processing the data are subject to a duty of confidence;
    - take appropriate measures to ensure the security of processing;
    - only engage sub-processors with the prior consent of the controller and under a written contract;

Prettys

Embedding compliance – systems and policies

- assist the controller in providing subject access and allowing data subjects to exercise their rights under the GDPR;
- assist the controller in meeting its GDPR obligations in relation to the security of processing, the notification of personal data breaches and data protection impact assessments;
- delete or return all personal data to the controller as requested at the end of the contract; and
- submit to audits and inspections, provide the controller with whatever information it needs to ensure that they are both meeting their GDPR obligations, and tell the controller immediately if it is asked to do something infringing the GDPR or other data protection law of the EU or a member state.

Embedding compliance – systems and policies

Relationships with others

From who do we receive data?

- Are we lawfully processing that data?
- Do we provide privacy information notices?
- What do the data providers expect from us?

Prettys

Embedding compliance – systems and policies

New systems and initiatives – Data Protection Impact Assessments (DPIAs)

When do I need to conduct a DPIA?

- using new technologies; and
- The processing is likely to result in a high risk to the rights and freedoms of individuals ; or

(Processing that is likely to result in a high risk includes (but is not limited to):

- systematic and extensive processing activities, including profiling and where decisions that have legal effects – or similarly significant effects – on individuals.
- large scale processing of special categories of data or personal data relation to criminal convictions or offences.

  This includes processing a considerable amount of personal data at regional, national or supranational level; that affects a large number of individuals; and involves a high risk to rights and freedoms e.g. based on the sensitivity of the processing activity.)

- Large scale, systematic monitoring of public areas (CCTV).

Prettys

Conclusions and questions

Contact us

Kelly Sayers
Partner and Head of Employment Services

ksayers@prettys.co.uk
Tel: 01473 298291

Matthew Cole
Partner

mcole@prettys.co.uk
Tel: 01473 298221

Vanessa Bell
Senior Associate

vbell@prettys.co.uk
Tel: 01473 298208

Emma Loveday-Hill
Associate

elovedayhill@prettys.co.uk
Tel: 01473 298266

Laura Pharez-Zea
Associate

lpharezzea@prettys.co.uk
Tel: 01473 298250

Sheilah Cummins
Associate

scummins@prettys.co.uk
Tel: 01473 298226

Prettys