sportscotland SGB Briefing Paper on the key changes under the GDPR

Driven by partnership

Harper Macleod LLP

Introduction

The General Data Protection Regulation (EU) 2016/679 (the GDPR) will directly apply in EU Member States from 25 May 2018. The GDPR replaces current data protection law and will be transposed into UK law by the new UK Data Protection Bill (the Bill), which will replace the Data Protection Act 1998 (the DPA).

Key Definitions

Definition	Examples
"Personal data" means any information relating to an identified or identifiable natural person (a "data subject").	Name, address, date of birth or email address of members, athletes, participants, employees, volunteers or parents.
"Processing" means any operation performed on personal data (including automated operations), including collecting, storing, consulting, using, disclosing, amending, deleting, etc.	Asking individuals to complete a form online, inputting their information into a database, sending communications, etc.
"Special categories of personal data" means data revealing a natural person's:	Racial or ethnic origin; political opinions, religious or philosophical beliefs; trade union membership; genetic or biometric data for the purpose of uniquely identifying a natural person' data concerning health or data concerning a natural person's sex life or sexual orientation.
"Controller" means the person who determines the purposes and means of processing personal data.	The organisation that decides how and why personal data is processed – usually the SGB. If an organisation is required by law to process personal data then it must be the controller.
"Processor" means the person who processes personal data on behalf of the controller.	Suppliers (including Azolve, IT service providers, etc.) and SGBs in certain cases.

Data protection principles

Personal data shall be:

1. processed lawfully, fairly and in a transparent manner in relation to the data subject;
2. collected for specified, explicit and legitimate purposes and not processed in a way that is incompatible with those purposes;
3. adequate, relevant and limited to what is necessary in relation to purposes;
4. accurate and kept up-to-date (where necessary) with reasonable steps to rectify or delete inaccurate personal data without delay;
5. kept in a form which can identify data subjects for no longer than necessary for purposes; and
6. processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Legal basis for processing

The GDPR sets out the grounds for lawful processing of personal data:

Personal data	**Special categories of personal data**
Data subject has given consent to the processing.	Data subject has given explicit consent to processing.
Necessary for performance of contract to which data subject is party or at request of data subject prior to entering into contract.	Processing is necessary for employment, social security or social protection law or collective agreement obligations.

Necessary for compliance with a legal obligation to which controller is subject.	Processing is necessary to protect the vital interests of a data subject or another individual where data subject is physically or legally incapable of giving consent.
Necessary in order to protect vital interests of data subject or another natural person.	Processing is carried out by a not-for-profit body with a political, philosophical, religious or trade union aim provided the processing relates only to members or former members (or those in regular contact re purposes) and provided there is no disclosure to a third party without consent.
Necessary for performance of a task carried out in public interest or in exercise of official authority vested in controller.	Processing relates to personal data manifestly made public by the data subject.
Necessary for the purposes of legitimate interests pursued by controller or by a third party, except where such interests are overridden by interests or fundamental rights and freedoms of data subject which require protection of personal data, in particular where the data subject is a child.	Processing is necessary to establish, exercise or defend legal claims or where courts are acting in judicial capacity.
	Processing is necessary for reasons of substantial public interest on basis of EU / UK law.
	Processing is necessary for preventive or occupational medicine purposes, for assessing employees' working capacity, medical diagnosis, provision of health / social care or treatment, or management of health / social care systems under EU / UK law or a contract with a health professional.
	Processing is necessary for public health interest reasons.
	Processing is necessary for archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes under the GDPR.

Privacy notices

Individuals have a right to be informed under the GDPR, which encompasses controllers' obligations to provide "fair processing information" through a privacy notice. SGB's privacy notices must include:

- identity and contact details of SGB and data protection officer (if appointed);
- purpose of processing and legal basis;
- legitimate interests of SGB or third party, where applicable;
- any recipient or categories of recipients of personal data;
- details of transfers to third country (outside the EU) and safeguards;
- retention period or criteria used to determine retention period;
- existence of data subject's rights, including the right to lodge a complaint with the Information Commissioner's Office; and
- right to withdraw consent at any time, where relevant.

Controllers must ensure that data subjects are provided with the information set out above at the point of collecting personal data – for example, within an application form to be completed by a data subject or on a website.

Consent

The GDPR requires that consent:

- must be a clear affirmative action: opt-in rather than opt-out and no pre-ticked boxes;
- should be separate from other terms and conditions and not a precondition of signing up to a service;
- provides granular options for different processing operations; and
- is easy to withdraw.

Under the GDPR, consent will not be appropriate unless the SGB can offer individuals a genuine choice over how their personal data is processed. For example, where:

- the SGB would still process the personal data on a different lawful basis;
- consent is require by the SGB as a precondition for accessing its services; and / or
- the SGB is in a position of power over the individual (for example, an employee / employer relationship).

There will be many documents / statements out there with implied consent. For example, a statement providing that an individual "hereby consents to the use of my personal data by X by signing the declaration below…"

These statements will need to be reviewed to allow individuals to actively consent or replaced with an appropriate privacy notice including the information we have set out above.

Rights of data subjects

Subject access – provide a copy of personal data and information on processing. One month to respond

Rectification – includes new right to complete any incomplete data.

Right to be forgotten – erase all personal data held, including further processing.

Right to restrict processing – block or suppress processing of personal data.

Object to processing – broader rights to object to processing, depending on legal ground for processing.

Data portability – obtain all personal data in commonly used form, which permits further re-use by the data subject.

Data processing

Processors must be engaged by controllers under contracts with the provisions (stand-alone contract or part of wider contract) that stipulate that the processor:

- processes the personal data only on the controller's instructions;
- ensures that only persons subject to confidentiality provisions are authorised to access the personal data;
- takes all security measures required under the GDPR;
- does not engage another processor without prior specific or general written authorisation of the controller and notifies the controller of any intended changes re sub-processors. Sub-processors shall be subject to the same obligations under a contract and the processor fully liable for any breaches by any sub-processor;
- assists the controller to respond to requests exercising data subject's rights under the GDPR;
- assists the controller for ensuring compliance with the security, notifications to the ICO and data subjects re data breaches, data protection impact assessments and consultation with the ICO for high risk processing;
- deletes or returns the personal data to the controller at the end of the contract (at controller's discretion) and deletes existing copies unless require to be retained by law; and
- provides any information required by the controller to demonstrate compliance with its processing obligations under the GDPR and contribute to audits conducted by the controller.

Accountability principle
The GDPR requires controllers to be responsible for and be able to demonstrate compliance with the data protection principles – 'accountability'.

The measures controllers must take include:

- keeping records and documentation about processing activities;
- implement data security requirements and comply with security breach obligations;
- carry out and use, where appropriate, data protection impact assessments; and
- where appropriate, appoint a data protection officer.

Breaches and sanctions

Breaches:

- Personal data breaches are to be notified within 72 hours to the ICO and, where the breach puts individuals' data at risk, to the individuals concerned.
- Failing to notify a breach when required to do so can result in a significant fine.

Sanctions:

- Both controllers and processors are liable.
- Data subjects can sue for compensation and refer complaints against controllers based in any Member State to their own data protection regulator (the ICO in the UK).
- Increase in the highest level of fines of up to €20m or 4% of annual worldwide turnover (whichever is greater) for serious compliance failures.

Action plan for SGBs

1. Undertake data protection audit to identify the: categories of personal data and data subjects; uses of personal data; requirements for using the personal data; source of the personal data; and whether the personal data shared with any third parties.

2. Review existing forms, correspondence, websites, data protection statements: check if all documentation that asks for personal data includes a privacy notice, which meets the GDPR requirements and if all contracts include a data protection clause and amend to reflect the GDPR requirements if it relates to a processor.

3. Be prepared for data subjects to exercise their rights: set out procedures and responsibilities to comply with timescales and put in place procedures for audit trails and locating data.

4. Establish an accountability framework: implement / review data protection policies and procedures; set up procedure for maintaining records of processing activities; maintain audit trails; and date protection impact assessments.

5. Roll out data protection training: ensure that all individuals involved in processing personal data held by the SGB has a basic understanding of data protection and the SGB's obligations under the GDPR.

6. Adopt higher standards of data security.

7. Implement procedures for data protection breach management.

8. Consider cyber insurance.

9. Consider appointing a data protection officer: not an express requirement for SGBs but, if appointed, the DPO would need to comply with the GDPR provisions.

10. Do not wait until May 2018.

About us

Harper Macleod is a leading Scottish independent law firm that is driven to deliver.

Our growth and success is determined by your success, which is why we always try harder. We don't just see ourselves as lawyers, we see ourselves as problem solvers and business advisers, who focus on understanding your needs. We work side by side with you, using law as a tool to provide innovative solutions that are tailored to organisations and individuals.

It's this drive that sets us apart and delivers a better outcome for you or your organisation.

 harpermacleod.co.uk

 info@harpermacleod.co.uk

 @HarperMacleod

Glasgow
The Ca'd'oro
45 Gordon Street
Glasgow G1 3PE
t: +44 (0)141 221 8888

Edinburgh
Citypoint
65 Haymarket Terrace
Edinburgh EH12 5HD
t: +44 (0)131 247 2500

Inverness
Alder House
Cradlehall Business
Park Inverness IV2 5GH
t: +44 (0)1463 798777

Lerwick
St Olaf's Hall
Church Road, Lerwick
ZE1 0FD
t: +44 (0)1595 695583

Thurso
Naver House
Naver Road
Thurso KW14 7QA
t: +44 (0) 1847 630930

Harper Macleod LLP