# GEMTALK – Data Retention

## Process, Procedures and Policies

Ivana Bartoletti — Head of Data Protection and Data Ethics

Gemserv

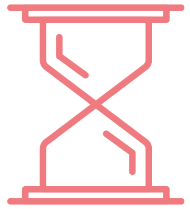
# Structure

- **Introduction to the Webinar**
- **Data Processing: Key Principles**
  - Principles for data processing
- **Data Retention: Process, Procedures and Policies**
  - Conducting a data mapping exercise
  - Governance and stewardship of data
  - How to comply with data minimisation
  - Relevant retention periods in various sectors:
    - General
    - HR
    - Finance
    - Marketing
- **Processes for data deletion, destruction and archiving**
- **Questions and Answers**

# Data Processing: Key Principles

# Principles for data processing

- Article 5 of GDPR sets out seven key principles:
  - Lawfulness, fairness and transparency
  - Purpose limitation
  - Data minimisation
  - Accuracy
  - Storage limitation
  - Integrity and confidentiality (security)
  - Accountability



# Lawfulness and Accuracy Principles

**Article 6** of GDPR sets six specific bases which should be relied upon to fulfil the lawfulness requirement.

Information on retention periods should be communicated in the Privacy Notice. This can be done in a table format, corresponding to the relevant data and legal basis.

The organisation's actual retention policy does not need to be made public.

For data retained for longer periods, ensure you comply with the obligation to keep it accurate, which may involve contacting the customer.

**Article 6 legal bases:**

- ❑ Consent;
- ❑ Performance of a contract;
- ❑ Legal obligation;
- ❑ Protection of vital interests;
- ❑ Task in the public interest;
- ❑ Legitimate interest

# Purpose Limitation

The purpose limitation principle prevents using personal data for new purposes if they are 'incompatible' with the original purpose.

Remember the following principles:

1. A Record of Processing Activities should determine the relevant purposes
2. Personal data collected for one purpose generally may not be used for a new, incompatible purpose
3. Consider a compatibility test for further processing
4. Consent may also be required for the additional use

Article 5 (1) (b) GDPR:
Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

# Purpose Limitation - Examples

**Requirements:** processing is *necessary* to:
(1) perform a data subject's contract, or (2) enter into a contract under a data subject's initiative.

***Example:*** A company collects CCTV monitoring of its premises for security purposes. It detects footage of a break-in and, after police open an investigation, provides the images to them.

***Example:*** An online campaigning organisation allows users to register with their email to receive updates on the progress of a petition. It then uses this information to target them with advertising.

*For the second option, consent would be required.*

# Data Minimisation Principle

Article 5 (1) (c):
Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

- The key element is that organisations should not process more than the minimum amount of data needed.
- This applies to collection, usage and storage.
- Consider that the personal data is **relevant** for that purpose.
- Evaluate that the information collect is **necessary** and not excessive.

***Example:*** Willy Wonka's factory offers free visits to members of the public that win a ticket. In order to carry out a risk assessment, the factory collects information on visitors on a form, including information about their age, health conditions, allergies and emergency contact details. The factory ensures this form does not have excessive or unnecessary sections or requirements.

# Storage Limitation

Storage limitation involves keeping data no longer (in terms of time) than necessary.

Article 5 (1) (e):
Personal data must be 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.

- Personal Data shall not be retained for a period longer than necessary for its purposes.
- Data no longer required should be removed by different methods:
  - Destruction
  - Retention
  - Archiving
- Introduce a policy outlining standard retention periods wherever possible
- Organisations should evaluate, perhaps annually or every six months, old records alongside the retention policy.

# Data Retention: Process, Procedures and Policies

# Conducting a data mapping exercise

Data mapping involves identifying types and locations of data, and how it flows throughout the organization and beyond.

Data Mapping should include :

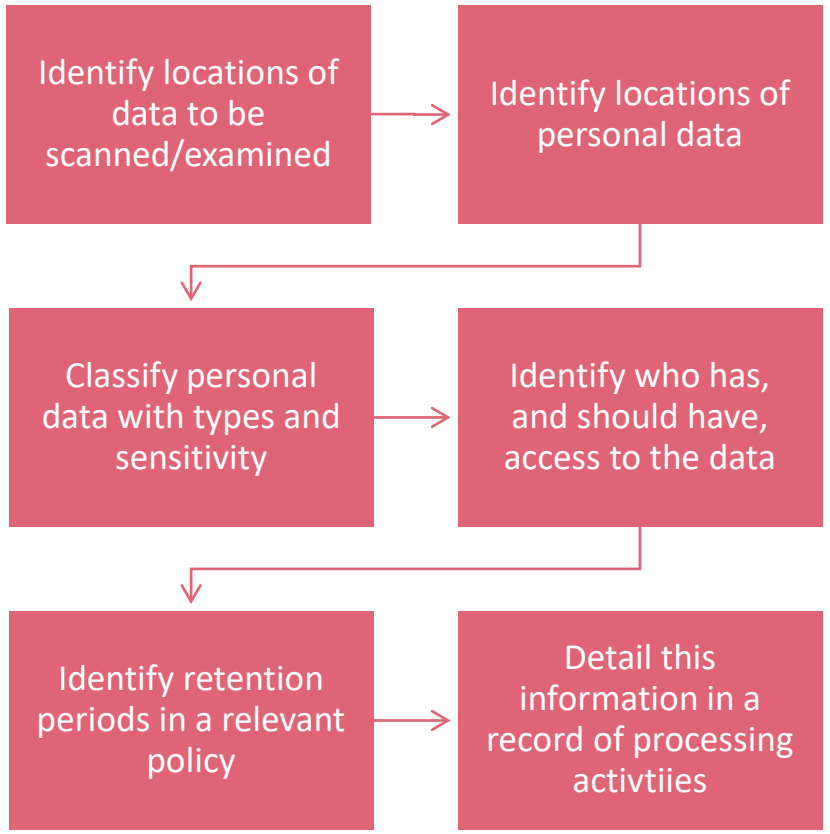
- The purposes of processing data (customer management, marketing, etc)
- The categories of the individuals involved (customers, employees, etc)
- The categories of personal data being processed (financial information, health data, etc)
- The categories of any recipients of the data (suppliers, etc)
- Details of any transfers to other countries
- How long the data will be kept for (retention periods)
- The technical and organizational security measures in place (encryption, access controls, etc)

Data mapping is required for a Record of Processing Activities.

It can also help in forming a Data Retention Policy and relevant periods.

# Conducting a data mapping exercise (continued)

**This explains how a data mapping exercise should work in practice:**



# Governance and stewardship of data

Data Stewards are responsible for business processes that involve personal data

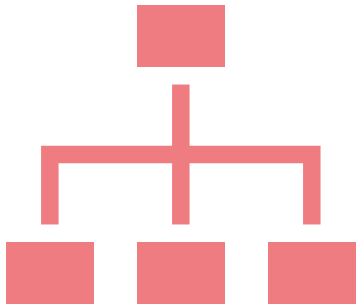
This includes:

- ❑ Responsibility for business processes involving personal data
- ❑ Stewardship and sign-off of assets and databases
- ❑ Assigning accountability to employees responsible for data assets
- ❑ Granting or restricting access to data
- ❑ Ensuring security measures are in place on databases or files

The DPO is responsible for ensuring compliance with data protection policies and other activities, but is not responsible for owning data or processes

# Governance and stewardship of data (continued)

These are some examples of data or process stewardship:



The IT Department will be responsible for providing support for the amendment and removal of data from systems.

The Data Protection Officer/DPO will oversee compliance policies, include for data deletion and amendment by the relevant Data Owners

The Marketing/Communications department will ensure that all the retention periods are met for data on most CRM systems and website.

# How to comply with data minimisation

The key element is that organisations should not process more than the minimum amount of data needed. This applies to collection, usage and storage.

This includes:

- ❑ Designing forms to include the minimum number of fields necessary
- ❑ Limit collecting information through monitoring or IoT devices
- ❑ If information is repurposed, see if all the data needs to be carried over

# How to comply with data minimisation (continued)

Here are some examples of using data minimisation in practice:

**Example.** An school is recruiting for a teaching position that involves working with you children. As such, it undertakes a criminal records (CRB) check into the applicant's background, and searches their LinkedIn profile, but does not record information from their Facebook page as the collection of such data would be excessive.

**Example.** An operator of mobile health apps collects information on users through sensors available on the phone. Although it collects information on distances walked and regularity of exercise, it does not profile users based on their location to suggest nearby stores and restaurants.

**Example.** An employer engages in monitoring of employee devices to ensure adherence to a code of conduct. It limits monitoring to device location, IP address and category of website viewed, without checking the content of emails or messages sent.

# Applicable retention periods in various sectors

Relevant retention periods can be provided from various sources, for example:

1. If there is a legal retention period specified in relevant legislation, this should be followed

2. If there is no legal retention period, consider supervisory authority guidance or industry best practice

3. If there is no legal retention period, consider how long the data is needed for the particular operation

4. If a new purpose is needed, a new retention period should either be identified or considered, and recorded

Keeping data ‘indefinitely’, even if this is a set period, is unlikely to be proportionate

It will always be necessary to specify ‘a’ period

# Where do the retention periods come from?

**Retention periods can come from: 1) Legal requirements; 2) Supervisory authority guidance; 3) Contractual requirements; 4) Operational requirements**

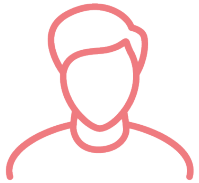
**Legal Requirements.** You should examine if your organisation is subject to any of the following:

- ❑ Health and safety legislation
- ❑ Immigration legislation
- ❑ Tax legislation
- ❑ Terrorism legislation
- ❑ Employment legislation

**Principally where consent and legitimate interest are relied on, you should:**

- Consider a legitimate interest assessment to decide what is fair
- Consider how long the project/operation will last

# Examples of determining periods



***Example: A***n organisation running a project for which volunteers are involved may delete personal data after the end of the project, apart from basic contact details to offer them future opportunities, if they opt-in.

***Example:*** For customer data, would they expect their data to be kept for years after the no longer buy your goods and services?

*These are examples of periods that can be determined.*

# Retention Periods: General

The following have been provided from various sources (supervisory authority guidance, best practice) as relevant retention periods:

CCTV monitoring records (guidance):
UK: 30 days
FR: 1 month
DE: 2 days

Photographs (best practice):
**Varies with each project**
**Suggested duration of the project**

Cookie IDs (guidance, best practice):
**Varies with each cookie, but:**
FR: Maximum 13 months

**Cookies:**

- ❑ **Consider if 'session cookies' are more appropriate**
- ❑ **Consider if using cookies with longer retention periods is necessary e.g. for targeted advertising**
- ❑ **Avoid using third-party cookies with long retention periods**

# Retention Periods: HR

The following are good examples of retention periods:

Data of rejected job applicants:
UK: 6 months post-campaign (guidance)
NL: 4 weeks post-campaign (guidance)

Immigration documents (IDs, passport, etc.):
UK: 2 years (legal)
NL: 5 years (legal)

Payroll records:
UK: 6 years after the relevant FY (legal)
FR: 5 years after the relevant FY (legal)

Accident records:
**Varies with each, but:**
UK: Up to 40 years (legal)
FR: Standard – 10 years. Up to 40 years for specific exposure (legal)

# Retention Periods: Finance

The following are good examples of retention periods:

Tax returns and records:
UK: 6 years after the relevant FY (legal)
FR: 6 years after the relevant FY (legal)

Customer invoices and receipts:
UK: 6 years after the relevant FY (legal)
NL: 7 years after the relevant FY (legal)

VAT records:
UK: 6 years after the relevant FY (legal)
FR: 6 years after the relevant FY (legal)

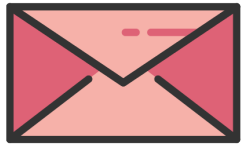
# Retention Periods: Marketing and Events

The following have been provided from various sources (supervisory authority guidance, best practice) as relevant retention periods:

Potential clients/customers etc.:
UK: 2 years from opt-in/opt-out consent (guidance)
FR: 3 years from opt-in/opt-out consent (guidance)

Customer relationship information:
UK: 2 years from the end of the customer/client relationship (guidance)
NL: 3 years from the end of the customer/client relationship (guidance)

Dietary requirements at events:
**Suggested duration of the event**
**Longer periods may be required for repeat customers (e.g. duration of their relationship)**



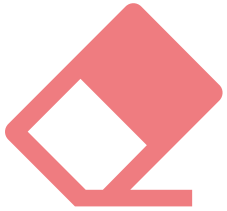
# Retention, Destruction and Archiving

**Once data has reached the end of its purpose, or the relevant specified retention period has elapsed, organisations can do one of the following:**

**Destroy the relevant records**

**Archive the data – if a further retention period is required**

**Anonymise the records - e.g. for statistical purposes**



# Data destruction

Records are to be destroyed under secure conditions

**The following can be useful guidance in data destruction:**

- Ensure that backups are deleted as well as originals
- Paper records and hard-drives can be shredded.
- From commercial organisations that carry out data shredding/destruction procedures, receive a certificate of destruction.

# Anonymisation

Anonymisation must be subject to specific procedures

Anonymisation can be accomplished by removing possible identifiers.

Alternatively, techniques such as encryption and obfuscation can be used.

**Example:** An employer collects information on the location and travel time of employees for a particular project, to compensate their expenses. Following the end of the project, the company wishes to keep this data for statistical reporting. Anonymisation is a useful tool to accomplish this.

# Archiving

Archiving could be useful where:

- ❑ There is a legal obligation to keep data for a fixed period
- ❑ The data records do not need to be readily accessed on a day-to-day basis

**Example:** An employer maintains employee data, such as bank details, for monthly salary and benefits payments. When the employee leaves the company, it still needs to retain the data for financial obligations, so it uses the database to archive the data.

# Any questions?

# Thank you for listening

Please feel free to contact:
dataprotection@gemserv.com

Gemserv

INVESTORS IN PEOPLE | Gold Until 2020

bsi. ISO/IEC 27001 Information Security Management

GlobalGROUP ISO 14001 UKAS MANAGEMENT SYSTEMS 0039

LLOYD'S REGISTER LRQA ISO 9001 UKAS MANAGEMENT SYSTEMS 001

CYBER ESSENTIALS PLUS