Data Security/Information Governance/General Data Protection Regulations (GDPR)

Claire Penellum St Austell & District

Emergency Preparedness, Resilience & Response Manager – NHS Cornwall and Isles of Scilly ICB

Director Owner – Simba360 Ltd

Non-Executive Director – Rewind Radio (Southwest)

Board Chair – Inspiring On Healthcare group of companies

Former Information Governance/Data Protection Manager – Community Health Services, Cornwall

‘If’ by Rudyard Kipling

If you can keep your head when all about you are losing theirs…. …. ….

…. Then you probably haven’t understood the severity of the problem!

Session Aim - To bust the myths and fear around GDPR

- To be an interactive session
- Be open and honest – safe space
- **Say it LOUD – I am legally deaf**
- Presentation will be made available
- Post today an offer of support/drop-in FAQ sessions via Zoom or MS Teams.
- Sharing of documentation produced for St Austell & District Club (scheduled to be completed by end January 2024).
- Online GDPR training session for officers/clubs (From January 2024).

Clubs are responsible for their GDPR arrangements.

SIGBI guidance

SIGBI Ltd Online Security Guidance 2022	A Club's Data Protection Policy – Updated 12 April 2023	A Club's Guide to Data Protection – Updated 28 July 2023	A Club's Privacy Notice – Updated 12 April 2023	Clubs – Data Audit Form – April 2018	Clubs – Data Breach Policy – April 2018	Clubs – Data Protection Complaints Process – April 2018	Clubs – Letter re Data Protection – April 2018	GDPR frequently asked questions	SIGBI Data Protection Protocols – Updated 12 April 2023	SIGBI Privacy Notice – Updated 12 April 2023

Privacy or Processing Notices – ensuring compliance

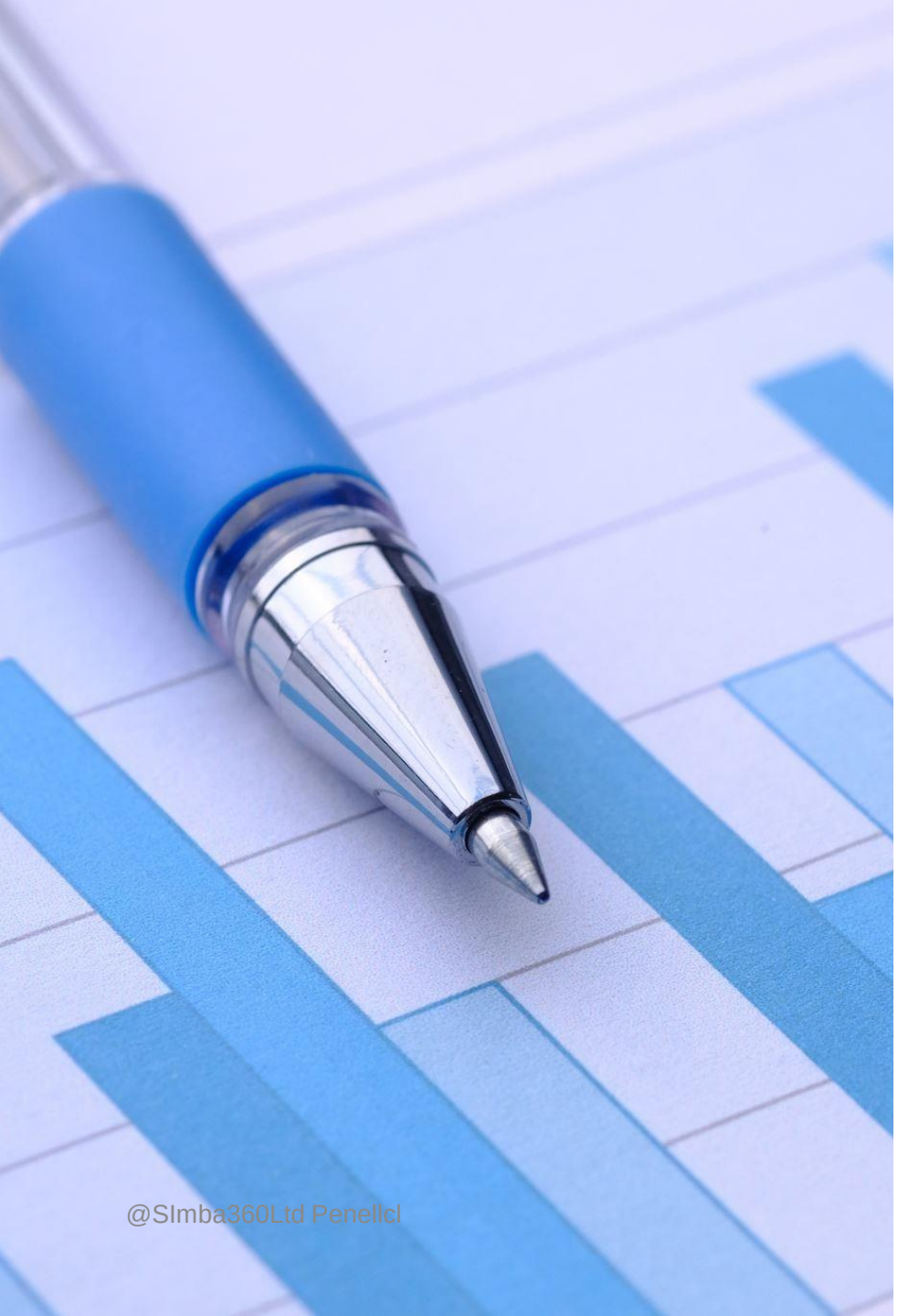
These are synonymous and both refer to statements provided to data subjects **at the point of data collection**

Privacy policies often mean the same thing but can refer to a document that is only used internally by a club to detail its rules and practices for dealing with personal data.

We all hold personal data so are required to have a privacy notice, which is sometime known as ‘fair processing information’, ‘privacy information’, or a ‘privacy policy’.

Information provided to data subjects must be:

- Concise, transparent, intelligible and easily accessible; and
- Written in clear and plain language.



Key considerations for privacy notices

- The lawful basis on which you are relying in order to process particular categories of data. Such bases can include processing based on:

1. The data subject's consent;
2. The clubs' legitimate interests; or
3. The performance of a contract.

There is a level of technicality to this particular consideration.

You need to review and update the notices regularly.

Identifying all data processing activities

Data processing as defined by the EU is the:

“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 of personal data”.

Privacy Notices – What should they say/include

- How the club use your information
- Why we are collecting your data
- The categories of information that we may collect, hold and share (personal information and characteristics (gender, ethnicity, language, nationality, country of birth))
- Storing your data
- Who do we share your information with
- Your rights – https://ico.org/for-the-public/is-my-information-being-handled-correctly/
- Promotional communications (opt out information)
- Marketing (opt out information)
- Web pages
- Social media
- Security and performance (use of 3rd party services for publication of blogs and materials
- Frequency of renewal
- You may end up with a few versions depending on the information source.
- Make your own privacy notice
- Video: Data protection explained in three minutes

ACTIVITY – NEXT SLIDE

Activity - Data Mapping

- What/whose data do you hold?
- Where/Who?
- In one place or have individuals got a variety of versions?
- Historical data – Housekeeping. Are you doing it and how often?
- How do you know what the most up to date version is?
- What forms/paperwork do you need to add a privacy notice to?

- **Data flow mapping** – identifying if information can be connected to an identified or identifiable individual, including information such as:
  - Names
  - Identification numbers
  - Online identifiers
  - Phone numbers
  - Addresses
  - Card numbers or bank details
  - Appearance
  - Location data
  - Ethnic, religious, genetic, physiological, social, or other commercial identifiers.

Data Processing

Collect data processing locations – everyone in the club to explain the data processing they do (or the data they hold)

Include historic data – people who have left the club etc.

What will be your daily, monthly and yearly tasks?

How will you check/audit to ensure you are compliant?

- Data collection – Purpose, source, legal basis, location, and consent for the collected data.
- Data Use: Why and how will the information be used.
- Data Storage: The security measures, conditions, format, length of time the data will be kept.
- Data transfer: Locations and parties to which data is transferred, purpose for the transfer, security measures around the transfer.

If you're gathering this information manually, the best way to organise it is with some kind of spreadsheet. That will help you keep track of each piece of data and make it easier to cross-reference details later.
For example, the following spreadsheet demonstrates how you might organize a simple data map using the UK's ICO accountability tracker.

Data Processing

Look for gaps

Places where you don’t have all the information you need to determine if you’re in compliance.

Data processes that aren’t compliant.

Missing transfers.

Missing responsible parties.

Vague, inaccurate, or conflicting processes.

Generate your report for action

Completed data mapping with timescale for action and assigned individuals.

Repeat and Maintain

This is a continuous process – rinse and repeat.

It’s good practice to update your data maps once a quarter to keep them from becoming too out of date.

What is contained in the Data Map?

Type: What kind of data are you collecting? For example, are you collecting names, location data, IP addresses, other identifiable information, or just site usage details like links clicked?

Sensitivity of data: Article 4 of the GDPR specifies that personal data is any kind of information that's directly related to an identifiable natural person. If the data you're collecting can be traced back to a specific person, it's considered personal and subject to the GDPR.

Data source: How are you collecting your data? Are you gathering it directly from visitors or compiling data from external sources? You need to specify your sources in the data map.

Purpose of collection: You may only collect data for a limited number of purposes under the GDPR. Clarifying why you're gathering each piece of information in your data map can help you better understand whether you comply with the regulation.

Data usage: What are you using information for? This information is critical to managing your disclosures properly.

Storage period: Data retention is strictly limited by the GDPR depending on the type of data in question. Naming your storage period will help you spot if you're keeping data too long.

What is contained in the Data Map?

Storage location and conditions: Where does your data get stored? Is it held onsite or in an offsite data center? Is it ever converted to a paper format? You need to know **how you're storing data** if you want to manage it properly.

All data transfer destinations: You likely transfer data both internally and externally during the ordinary course of business. Track exactly where each piece of data gets sent to build the connections of your map.

Locations of external vendors receiving any data: If you transfer data to external vendors or international locations, where in the world are those vendors located? Vendors outside the EU aren't **held to the same standards** as EU businesses, so that can make consumer data less secure.

Data transfer protocols to external vendors: How is the transfer completed when you transfer information? What security protocols are in place? Security is essential to prove that you properly protect data.

Duties

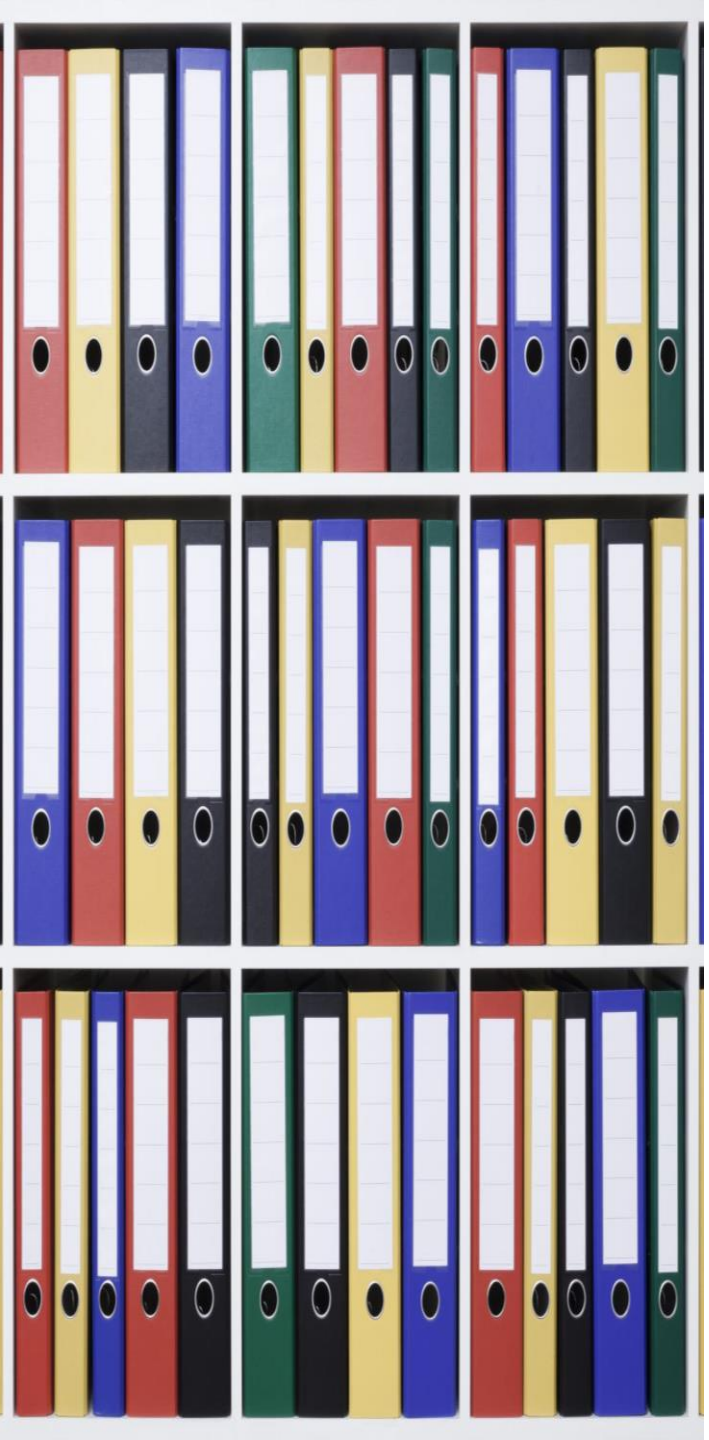
Part 3 of the DPA 2018 introduces a duty on all organisations to report certain types of personal data breach to the Information Commissioner. You must do this within **72 hours** of becoming aware of the breach, where feasible.

If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, you must also inform those individuals without undue delay.

You should ensure you have robust breach detection, investigation and internal reporting procedures in place.

Duties

- **What breaches do we need to notify to the ICO?**
  - You only have to notify the ICO of a breach if it is likely to result in a risk to the rights and freedoms of individuals. If left **unaddressed** such a breach is likely to have a significant detrimental effect on individuals. For example:
  - result in discrimination;
  - damage to reputation;
  - financial loss; or
  - loss of confidentiality or any other significant economic or social disadvantage.
  - In more serious cases, for example those involving victims and witnesses, a personal data breach may cause more significant detrimental effects on individuals.
  - You have to assess this on a case-by-case basis, and you need to be able to justify your decision to report a breach to the Information Commissioner.



What information must a breach notification to the Information Commissioner contain?

- You must include:
  - a description of the nature of the personal data breach including, where possible:
    - the categories and approximate number of individuals concerned;
    - the categories and approximate number of personal data records concerned;
  - the name and contact details of the data protection officer (if you have one) or other contact point where more information can be obtained;
  - a description of the likely consequences of the personal data breach; and
  - a description of the measures you have taken, or propose to take, to deal with the personal data breach and, where appropriate, of the measures you have taken to mitigate any possible adverse effects.

When do we have to tell individuals about a breach?

If a breach is likely to result in a **high risk** to the rights and freedoms of individuals, you must inform those concerned directly without undue delay.

A ‘high risk’ means the threshold for informing individuals is higher than for notifying the ICO.

The duty to tell an individual about a breach does not apply if:

you have implemented appropriate technical and organisational measures which were applied to the personal data affected by the breach (for example the data has been securely encrypted);

you have taken subsequent measures which will ensure that any high risk to the rights and freedoms to individuals is no longer likely to materialise; or

it would involve disproportionate effort.

Where a communication of a breach would involve disproportionate effort, you must make the information available to individuals in another, equally effective way, such as a public communication.

You may restrict the information, either wholly or partly, that you provide to individuals affected by a breach under certain circumstances. This is when doing so is a necessary and proportionate measure:

to avoid obstructing an official or legal inquiry, investigation or procedure;

to avoid prejudicing the prevention, detection, investigation or to prosecution of criminal offences or the execution of criminal penalties;

to protect public security;

to protect national security; or

to protect the rights and freedoms of others.

What information should we tell individuals who have been affected by the breach?

- You must give individuals information including:
  - a description of the nature of the personal data breach;
  - the name and contact details of the data protection officer (if relevant) or other contact point where more information can be obtained;
  - a description of the likely consequences of the personal data breach; and
  - a description of the measures you have taken, or propose to take, to deal with the personal data breach and, where appropriate, of the measures you have taken to mitigate any possible adverse effects.

Contact

- info@simba360.co.uk
- Personal: 07368 688753
- Work: 07768 251084