GDPR Part 2: Complying with the GDPR

Purpose

This Guide will show you how your organisation can comply with the GDPR. It should be read in conjunction with GDPR Part1: Understanding the Legal Framework and Key Legal Requirements.

Quick Summary

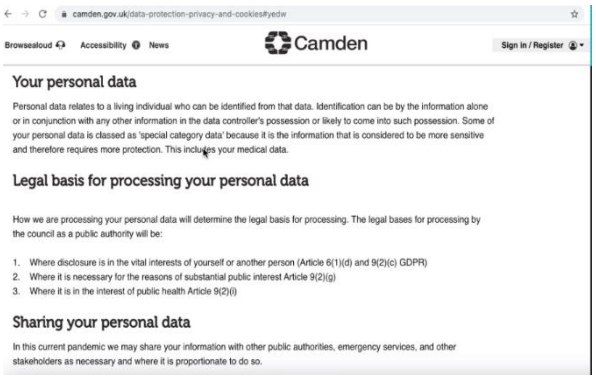
1. Organisations must always process personal data **lawfully, fairly, and in a transparent manner.**
2. Organisations can collect personal data only for **specified, explicit, and legitimate purposes**. They cannot further process personal data in a manner that's incompatible with those purposes.
3. Organisations can collect only personal data **that's adequate, relevant, and limited** to what's necessary for the intended purpose.
4. Personal data must be **accurate** and, where necessary, **kept up to date.**
5. Personal data must be **kept only for as long** as it's needed **to fulfil the original purpose of collection.**

Organisations must use appropriate **technical and organisational security** measures to protect personal data against unauthorized

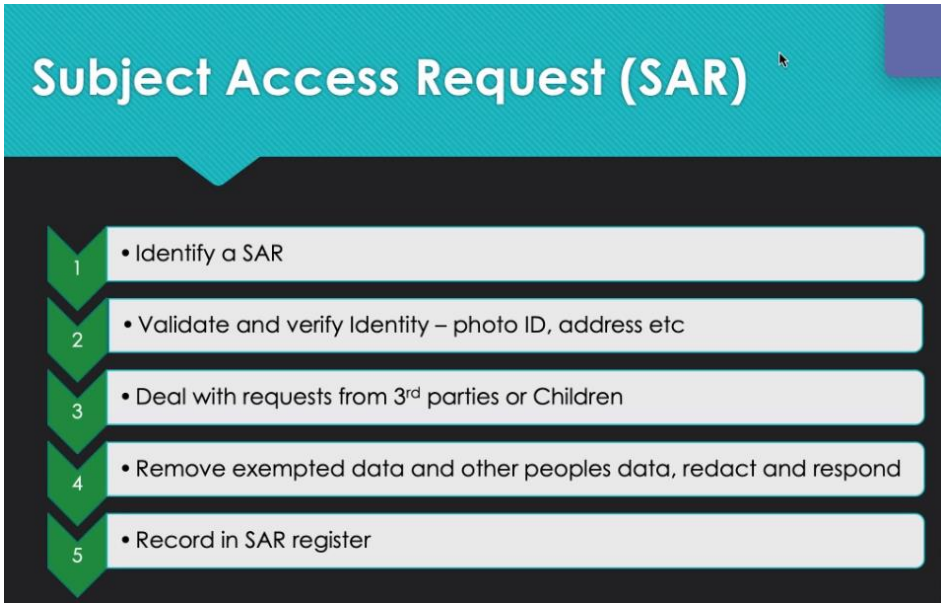
Privacy Notice

- **The Right to be informed is typically covered in a privacy notice. This is a public facing document that sets out how you process personal data and what Rights the Data Subject has with respect the personal information you hold on them.**
- Most common place for these is on an organisation's website, but this can also be linked to from other places e.g. when users sign up to use your services, when booking appointments, when filling out forms online etc. These can also be in paper form when they come to face-to-face activities.
- Must update privacy notice as things change e.g. sharing, type of data changes, legal basis changes etc.
- Must be provided at the time you collect the personal data, or at the earliest point after collecting the personal data (up to one month)
- Written in clear, plain English language, especially if to a child (you can use pictures)
- Concise, transparent, intelligible, easily accessible
- Free of charge!

- You can have one policy to capture the different services and ways data might be captured, but ensure all services are covered with the detail required; or you could have individual privacy notices for each service if this is totally different from the norm. this might be a clearer way of presenting the information for multiple and complex services that differ quite a bit in how data is processed.
- **Check out our Guide on drafting a Privacy Policy.**



Dealing with a Subject Access Request



- Individuals have a Right of Access to obtain a copy of their personal data as well as other supplementary information.
- You do not necessarily need to ask why they are asking for the information, although this can be helpful to narrowing down the search for the information they want.
- Ask to narrow down the scope e.g. individual mailboxes, date ranges, subject etc.
- Best practice to narrow down the scope
- Can be made in any form – verbally or in writing e.g. social media

- Role of organisations is to identify when SAR's are made, then to follow the agreed process to deal with the SAR
- Register and log the request and all associated actions relating to it.
- An individual is only entitled to their own personal data, and not to information relating to other people. This should be screened out before providing the data to the individual.
- Emails, documents etc are likely to be in email, shared drive on a server or in the cloud, in archives, social media, providers etc.
- Legal responsibility to identify that an individual has made a request to you and handle it accordingly
- Easy to lose track of all the places personal data might be kept!
- Can be painstaking job if lots of information, but only information that is *relevant* to the individual is required.
- Consent is NOT about reading the privacy policy. Consent is about what you consent your information being used for.
- Good practice is to outline what the user has consented to at the point that they provide consent.

Information you must provide:

- Purpose of your processing
- Categories of personal data concerned
- Recipients or categories of recipient you disclose the personal data to
- Retention periods for storing the personal data, or criteria for determining
- Right to lodge a complaint with the ICO
- Information about the source of the data, where it was not obtained directly form the individual
- Existence of any automated decision making
- Safeguards you provide if you transfer personal data to a third country or international organisation (must have something in place that identified what this agreement is)
- Most of this is already covered in your privacy notice and you can refer them back to the privacy policy.

Charging a fee

- Manifestly unfounded or excessive
    - Not really used that much
    - Can't rely on this as an excuse not to respond
    - Tends to be reserved for particularly complex requests with huge data sets relating to the individual.
    - You could offer to charge a fee or increase the response time to help deal with a request that is manifestly excessive.
    - Where you have already provided this information recently.

Response Times

- Must comply with a request without undue delay and at the latest within one month of receipt of request
- Can extend by a further two months if the request is complex or you have received a number of request from the individual.

- Calculate the response time limit from the day you receive the request (working day or not) until calendar date in the next month.
- Clock doesn't start ticking until the identity of the requester has been confirmed.
- If you have an approval system, make sure this is checked by someone else.

Data Protection Impact Assessment

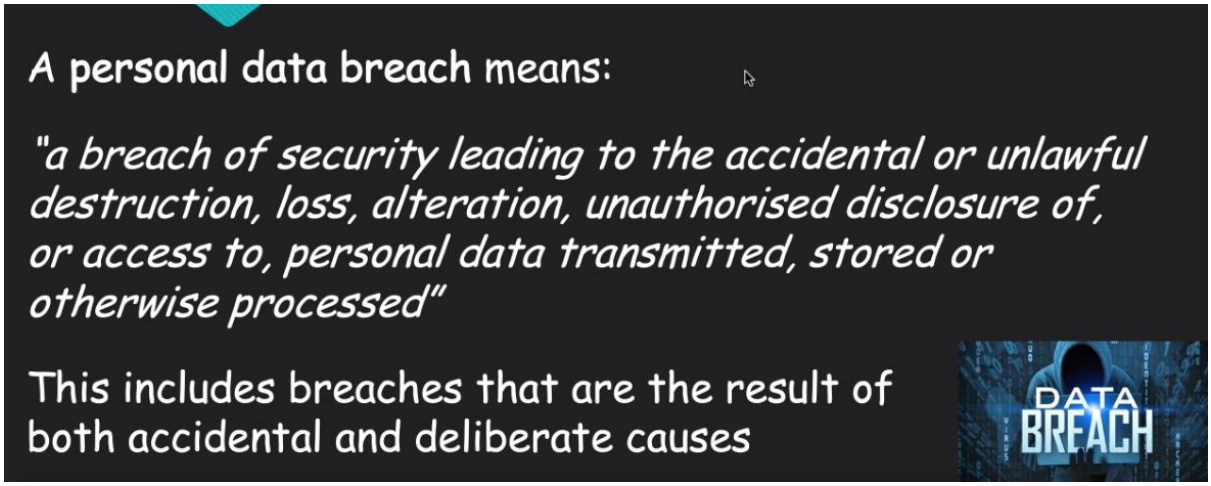
- Is essentially a risk assessment process to help you systematically anlayse, identify and minimise the data processing risks of a project or plan.
- Must do one if there is going to be a lot of processing of personal and sensitive information
- Always document reason if you decide not to do a DPIA.
- Can be fined if you don't do this at the time so always document, just in case.

Process

1. Identify the need –
    a. Might involve various roles, including people who know and use the data, develop the system etc.
    b. Have a coordinator but rarely a one person job
2. Describe the data processing that takes place
    a. What are you doing with the data?
    b. What information are you putting in? what happens next? What is the process for the flow of that information?
3. Consult stakeholders
    a. Double check with each party to check that the DPIA is properly conducted and identifying all known risks in advance
4. Assess Necessity and proportionality
    a. Review the data collection steps and check whether all is necessary
    b. Can you reduce the number of data points
5. Identify, assess and control risks

    a. Could be technical controls or administrative controls like training, writing guidelines etc.
6. Record the DPIA outcomes
    a. Can check the ICO template for this which is quite good
    b. Get this signed off by someone who has authority to approve risks (could be DPO, Director, trustees etc.).
7. Integrate the DPIA into the system
    a. Personal data should never go into a live system unless the risk assessment has been approved.
    b. Every time you think about new system or process, you should be thinking about doing a DPIA.

Incident Response and Data Breach



Key Points

- Key word here = breach of security
- Doesn't matter if this was accidental or not
- You must act accordingly if this happens

Examples

- sharing data with other people that should be kept confidential
- An unauthorised disclosure of an individual's data by that individual – accident or not
- Leaving documents on the bus
- Keeping the list of your members contact details in an unlocked cabinet in your office

Actions if you suspect a breach

- Report it ASAP
- To your Team lead / DPO
- To the ICO if considered a risk to individual
- You will need to notify the individual as well if high risk impact to individual. There may be other reporting requirements that you need to be aware of in the event of a breach

Demonstrating Compliance

- 7th principle of the UK GDPR – Principle of Accountability
- PIA/DPIA
- Privacy Policy
- Registered with ICO
- Data processor agreements logged
- Data audit with legal bases and retention period.
- Policies and procedures
- Registers of SAR and Data Breach
- Lawful basis and transparency for all personal data processing e.g. consent, privacy notice
- Technical and organisational measures
    - Locked cabinets
    - IT controls
    - Data Protection Policy
    - Information security policy
    - SAR policy and procedure etc.
- DPIA
- Record of Processing Activities (not the same thing as an informationa asset register, which would typically only contain a list of assets, their use and their owners)
- Training and awareness
- Processes to uphold privacy policy – SAR, breach management etc.
- Data Breach register
- Appoint a DPO where required (otherwise designate someone with responsibility for data protection)
-

Ask yourself:

- Do we have this in place?
- Is this up to date?
- Can we respond to an SAR if we get one?
- Do we have processes in place to handle x,y,z?

Key Takeaways

- Think security every time you handle personal data
- Know where and who to go to for assistance
- Do not collect personal data that you do not need
- Recognise when there is a subject access request
- Delete personal data when no longer needed
- Report data breaches asap
- Do not share personal data without checking that you are allowed to do so