TODAY’S PROGRAMME

1. GDPR in a nutshell
2. Principles and Rights
3. Where is your Data?
4. Consent
5. Subject Access Requests
6. Policies
7. Data breaches
8. Final checklist

1. GDPR in a nutshell

The GDPR in a Nutshell

- The GDPR (EU General Data Protection Regulation) affords a coherent and thorough personal data privacy law across all EU member states.
- GDPR aims to prevent security breaches.
- GDPR aims to prevent loss of personal data.
- Affects any organisation that offers goods or services or monitors the behaviour of EU Citizens.
- Replaces the Data Protection Directive 95/46/EC.
- Significant penalties for breaking the regulation.

The GDPR in a Nutshell

- GDPR will be the lawful benchmark that all organisations who process or store PII (personal identifiable information) must adhere to.

- The GDPR is a Regulation. It has been approved by the European Parliament and is, therefore, Law!

- Must be compliant from 25th May 2018.

- There are 99 Articles split into 11 Chapter and 173 Recitals.

- Consequences of failure - reputation, loss of earnings, fines etc.

Principles and Rights

Principles

1. Legality, transparency and fairness.
2. Purpose limitation.
3. Minimisation.
4. Accuracy.
5. Storage limitation.
6. Integrity & Confidentiality.
7. Accountability.

Rights

1. The right to be informed.
2. The right of access.
3. The right to rectification.
4. The right to erasure.
5. The right to restrict processing.
6. The right to data portability.
7. The right to object.
8. Rights in relation to automated decision making and profiling.

Fines
€20M or 4%

- Breaching the principles, including consent.
- Obstructing Data Subject’s rights.
- Non-compliance of data outside of the EEA.
- Non-compliance with an order by the Supervisory Authority.
- Non-compliance with an order, or temporary or definitive limitation on processing, set by the relevant Supervisory Authority,
- Failure to provide access in Violation of Article 58(1) (to Supervisory Authority).

Fines €10M or 2%

- Child consent
- Processing not requiring identification
- Data Protection by Design & Default
- Representatives of Data Controllers not established in the European Community (EC)
- Processing
- Co-operation with the SA
- Data Security
- Notification of breaches to the SA
- Communication of breaches to the Data Subject
- Prior Consultation
- Data Protection Officer
- Monitoring
- Certification

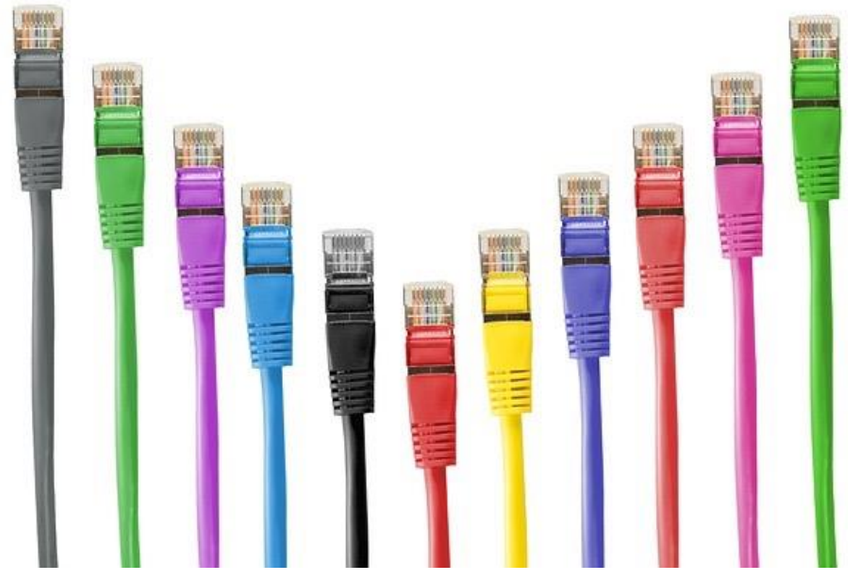
What's in it for us, the Data Subject?

- Generate Customer Confidence.
- EU single market rather than 28 markets each with different regulations.
- Instil confidence when using online services.
- Put us back in control of our PII. It gives all EU citizens more control over their data.
- PII has a **value** and has been **exploited**. GDPR grants people rights and places the obligation on the organisations that hold our data to protect it.

GDPR Applies to:-

All processing of personal data by just about any means.

Applies to all EU Citizens and those of the EEA and organisations outside the EU that offer goods or services to individuals in the EU.



2. Principles and Rights

Principles and Rights

Principles

1. Legality, transparency and fairness.
2. Purpose limitation.
3. Minimisation.
4. Accuracy.
5. Storage limitation.
6. Integrity & Confidentiality.
7. Accountability.

Rights

1. The right to be informed.
2. The right of access.
3. The right to rectification.
4. The right to erasure.
5. The right to restrict processing.
6. The right to data portability.
7. The right to object.
8. Rights in relation to automated decision making and profiling.

(1a) Legality Principle

- PII must be processed in accordance with the rules and guidelines of GDPR.

- Whilst doing so, an organisation must specify the grounds upon which it is processing PII.

- You must have a Lawful Processing Condition

These are:-

1. Consent
2. Performance of a contract
3. Legal (business) Obligation
4. Vital Interest
5. Public Interest
6. Legitimate Interest
7. Official Authority

Special categories

- Racial / Ethnic

Political Opinion / Affiliation

Religious or Political Beliefs

Trade Union Membership

Genetic / Biometric Data

Health Related

Sex- life / Sexual Orientation

Differences are:-

1. **Explicit** Consent
2. Vital Interest
3. Public Interest
4. **Made public by the Data Subject**
5. **Public health and health of DS**
6. **Employment**
7. **Member groups**
8. **Legal Claims**
9. **Archiving/stats/research**

(1b) Transparency Principle

- You must inform the data subject, clearly and thoroughly, the way you are processing their data

Must be in an accessible format

Provide for FREE

(1c) Fairness Principle

- to be treated fairly

rights adhered to
1 month to respond
a right is not a guarantee

(2) Purpose Limitation Principle

Quite simply……

Only use the data for the purpose you took it for

(3) Minimisation Principle

Only collect data that is… relevant, adequate and limited to what you need it for.

(4) Accuracy Principle

- Must be up to date

Avoid storing old data

Erase or rectify inaccurate data

(5) Storage Limitation Principle

Don’t keep for longer than necessary with exception of….

- Archiving purposes in the public interest
- Scientific or historical research
- Statistical

(6) Integrity and Confidentiality Principle

- Data must be processed in a manner that ensures appropriate security.

Organisational rules, and technical systems need to be considered.

Protect against unauthorised people accessing data.

(7) The Accountability Principle

- Data Controller and Data Processor must prove compliance with GDPR Principles.

GDPR requires businesses to show they are compliant.

ICO (our SA) can audit businesses.

Rights of the Data Subject

1. The right to be informed.
The right of access.
The right to rectification.
The right to erasure.
The right to restrict processing.
The right to data portability.
The right to object.
Rights in relation to automated decision making and profiling.

Must I always obey?

WHY?

- Public interest.

Public health.

Conform to legal obligation.

If you do reject - reason,
explain to Data Subject,
inform rights to contact SA.

3. Where is your data?

What is PII?

- GDPR article.4.(1) defines personal data as:-

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

Note: This is not a definitive list.

What is data?

- email addresses
- home addresses
- date of birth
- NI number
- telephone number
- IP address
- genetic
- medical
- financial

Where does your data live?

Where does your data live?

Where is your data?

- server
- mobile phones
- are there duplicate copies
- spreadsheets
- cloud
- laptops
- usb sticks
- Google sheets and docs
- your own companies data collection system
- reports
- CRM’s
- subcontractors, temp staff, suppliers who hold data on your behalf.

4. Consent

You **must** determine and document your lawful basis for processing personal data.

These are:-

1. Consent
2. Performance of a contract
3. Legal (business) Obligation
4. Vital Interest
5. Public Interest
6. Legitimate Interest
7. Official Authority

What is affirmative action?

Clear affirmative action means someone must take deliberate action to opt in.

What is not affirmative action?

- Failing to opt out is not considered to be consent.
- You are not permitted to rely on silence, inactivity, default settings, pre-ticket boxes, or your general terms and conditions.
- You are not permitted to take advantage of inattention, inertia, or default bias in any other way.
- The importance idea is that all consent must be opt-in consent - there is no such thing as opt-out consent.

Examples of Affirmative Action from the ICO

An individual drops their business card into a prize draw box in a coffee shop. This is an affirmative act that clearly indicates agreement to their name and contact number being processed for the purpose of the prize draw. However, this consent would not extend to using those details for marketing or any other purpose.

An individual submits an online survey about their eating habits. By submitting the form they are clearly indicating consent to process their data for the purposes of the survey itself. Submitting the form will not, however, be enough to show valid consent for any further uses of the information.

An example of good practice is your own contact form

Contact us

Fill out the form below and your local **it'seeze** consultant will get in touch with you to discuss your website needs further

Name: *

Postcode: *

Phone: *

Email: *

How did you hear about it'seeze?

Please select

How can we help? *

An example of good practice with Newsletter opt-in

Choose your ASOS emails

We want every email you open from us to be something you're 100% into. That's why we're giving you the power to control what you receive from us. So now you can choose to be first in line for sales, preview the latest collabs, or get all the latest updates on the latest products (or all of the above). Plus, you can switch it up any time you like. Yep, you've officially got the power!

Tell us below, so we can bring all the ASOS goodness straight to your inbox.

CHANGE MY PREFERENCES ›

Here's what you enjoy now

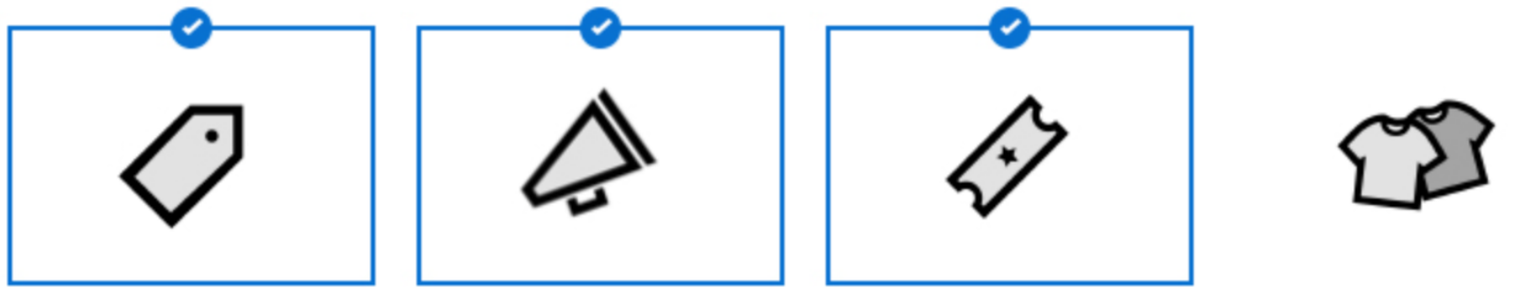
Scroll down to mix it up...

DISCOUNTS & SALES

NEW STUFF

YOUR EXCLUSIVES

ASOS PARTNERS



Sent by email, SMS, or both

KEEP SENDING ME THIS ›

CHANGE MY PREFERENCES ›

OPT ME OUT ›

5. Subject Access Requests

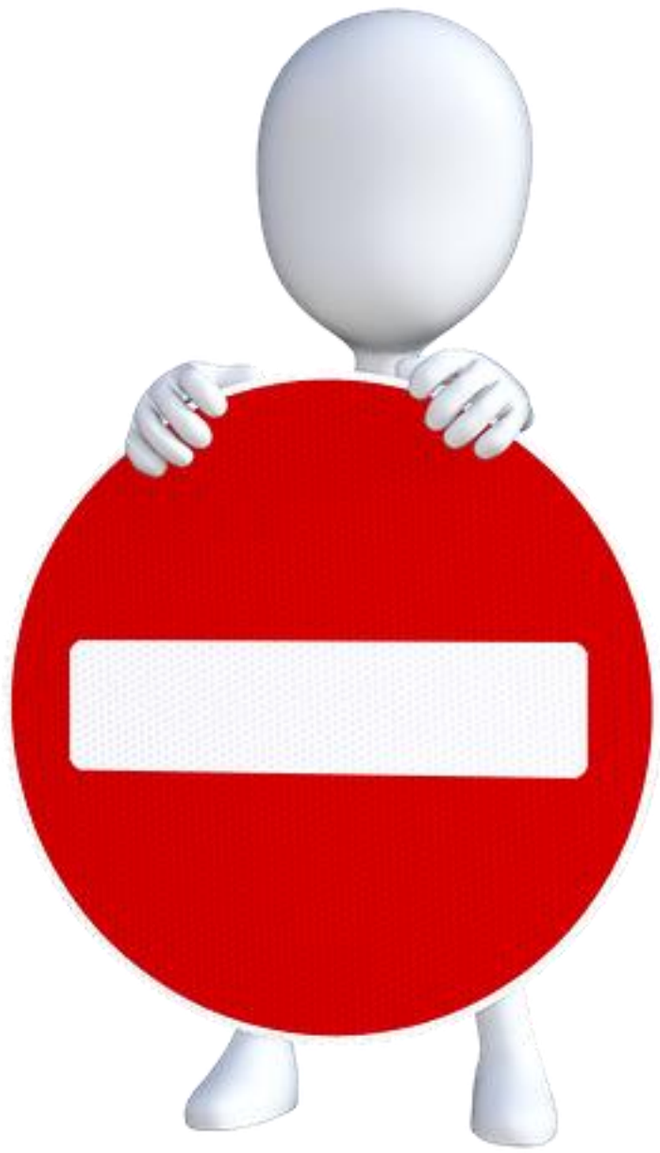
Subject Access Requests

- what data you hold on them.

what is your purpose for the data.
who holds a copy.
your retention policy.
rectification and erasure.
to stop processing.
Free and within 1 month.

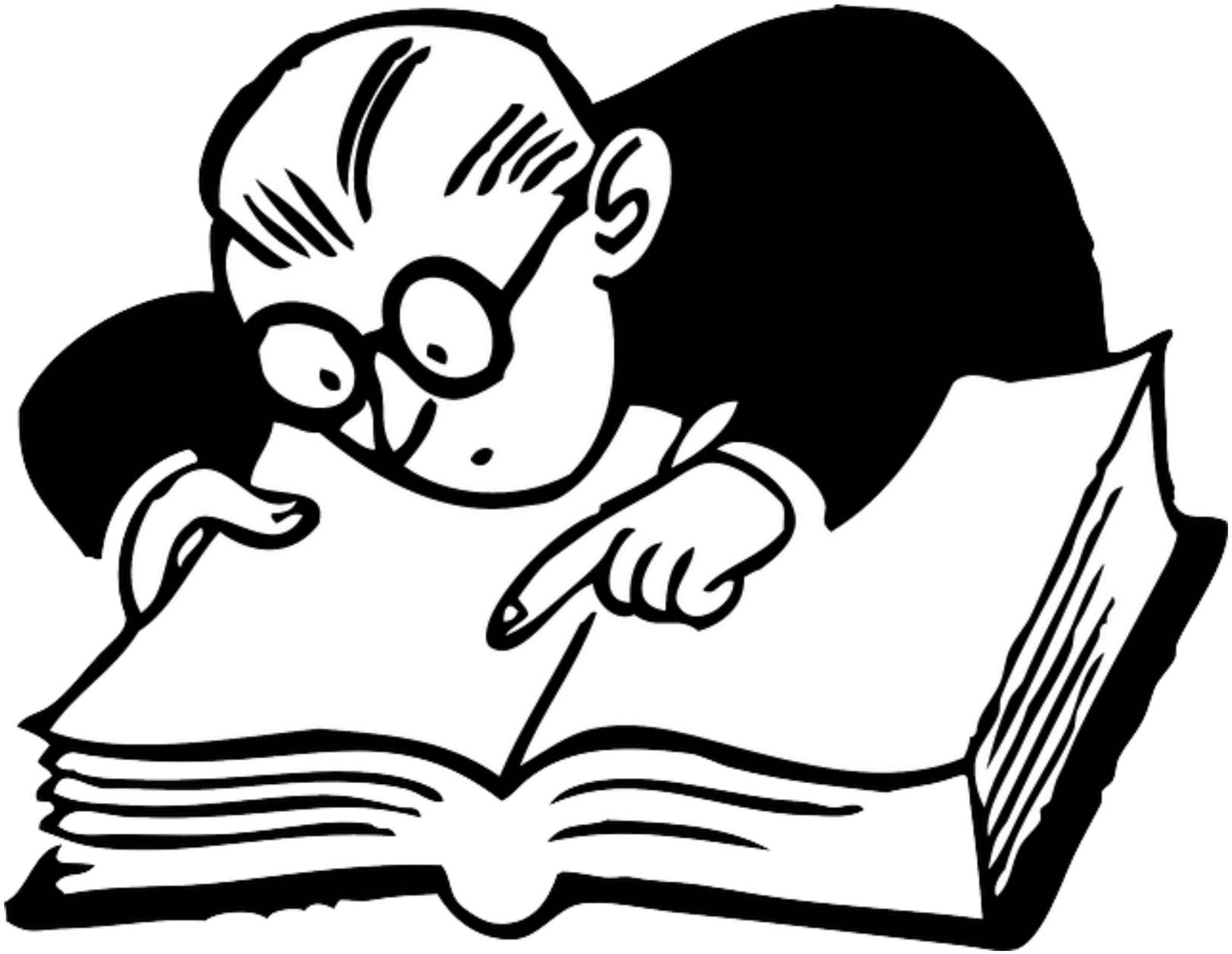
Subject Access Requests

- adversely affect the rights and freedoms of others unfounded or excessive demonstrate and defend your decision



6. Policies and Cookies

Policies and Terms Of Business



3 TOP POINTS:-

1. Tell them what you are doing with there data. Are you passing it on?

2. How are you securing the data? In accordance with the current Data Protection Laws.

3. Retention. How long will you keep their data?

7. Data Breach

Data Breach means…..

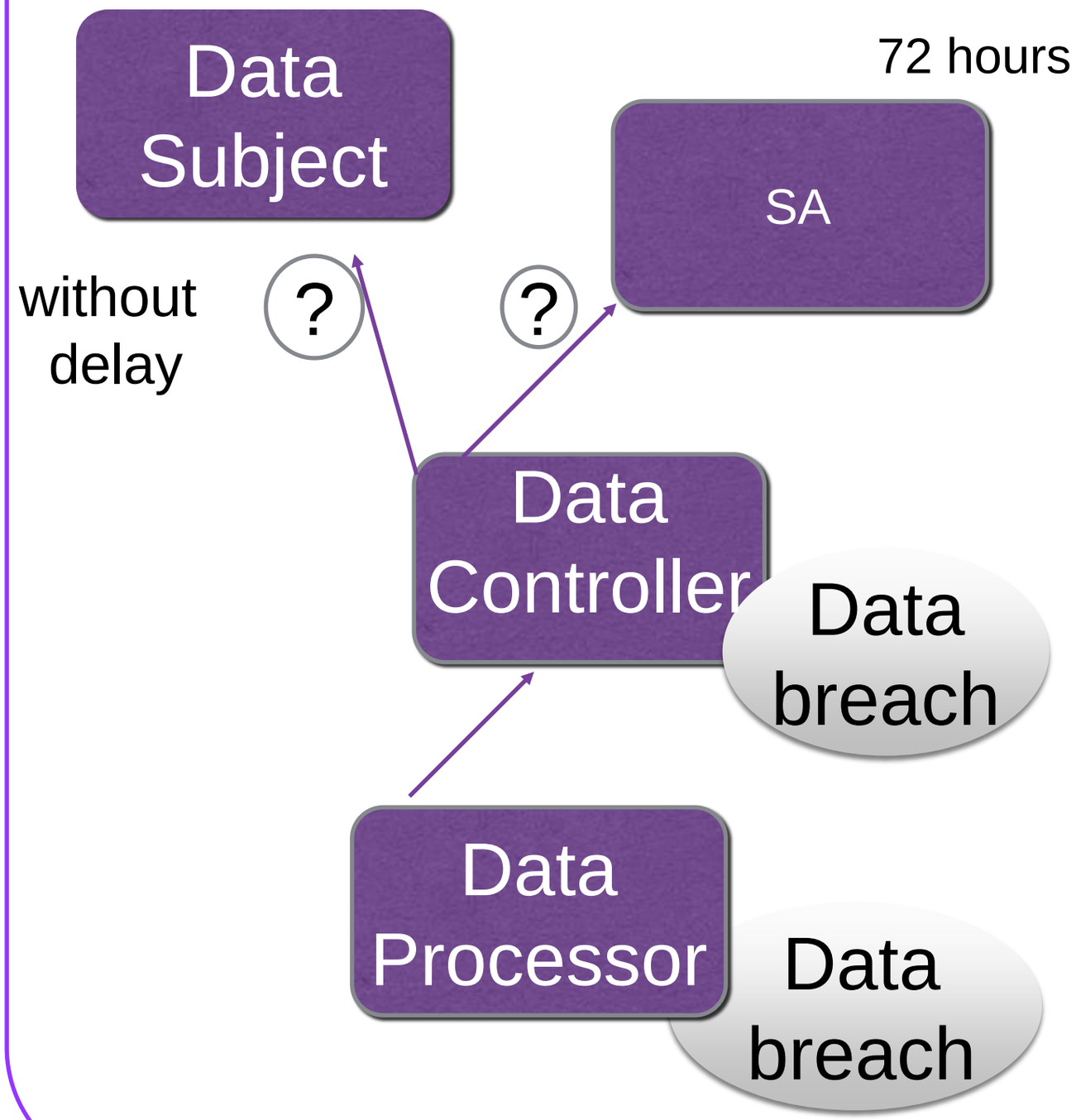
A breach of security leading to the……..

- accidental or unlawful destruction

loss
alteration without permission
sending data to an incorrect recipient
computing devices containing personal data
(lost/stolen)
unauthorised disclosures or access by a third party
access to personal data that has been transmitted,
stored or otherwise processed.

Pe

Who do I inform?



- Data Processor to notify the Data Controller

Data Controller to notify the SA (ICO)

Data Controllers to communicate the data breach to the Data Subjects

8. Final checklist

To store your data you need a legitimate reason and this easy principle is a great way of helping you focus on the different sets of PII your organisation has.

Need - Want - Drop

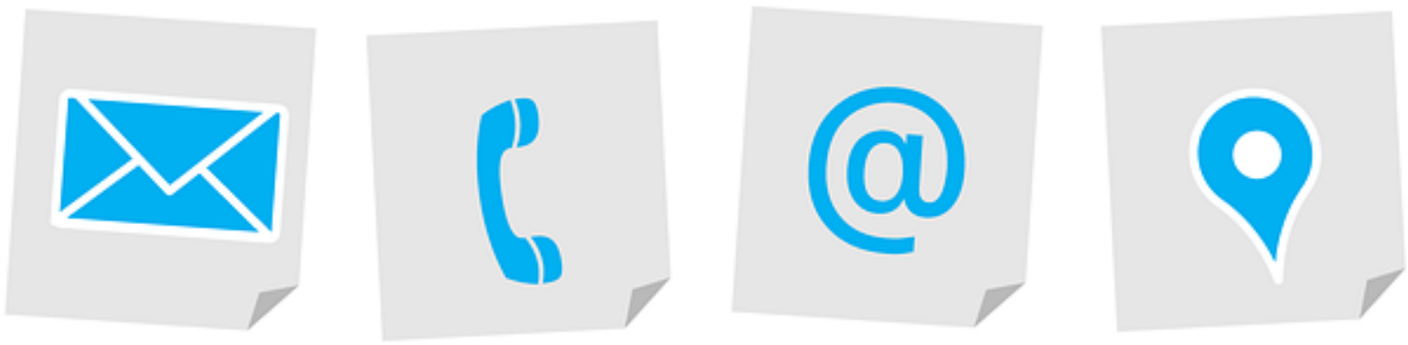
Need - Want - Drop

If not needed **DROP IT!**

Remember Asset -v- Liability

Leave with checklist

- Look at the data you hold.
- Make a Data Register - what, where, risks.
- Policies - cookie, privacy, data breach
- Do you need it? Need-want-drop
- Consent, consent, consent!



Lisa Wilson

Certified GDPR Practitioner

and Data Protection Officer

Ideea, Exeter Science Centre, Exeter

www.ideea.co.uk

07850070011

Don’t hesitate to get in touch