GDPR: Why should you care?

TERMINOLOGY

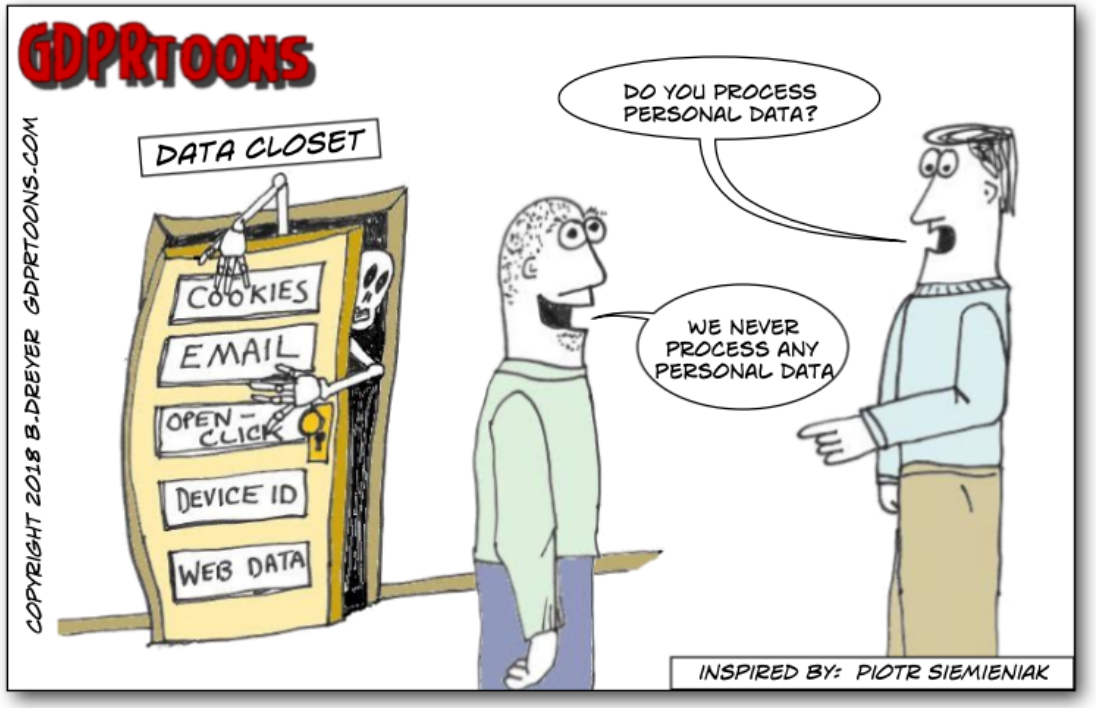
GDPR
A legal framework that sets guidelines for the collection and processing of personal information from individuals who live in the European Union (EU)

INFORMATION COMMISSIONER'S OFFICE
An independent regulatory office in charge of upholding information rights in the interest of the public in the UK.

DATA PROTECTION OFFICER
Independent data protection experts who are responsible for monitoring an organisation's compliance.

PERSONAL DATA
Any piece of information that someone can use to identify a living person.

TYPES PERSONAL DATA



PERSONAL DATA

- Name
- Email Address
- National Insurance Number
- Address (Home or Business)
- Postcode
- Date of Birth or Age
- Employee Number
- Gender
- Tax/Pension Records
- Marital Status
- Citizenship

SPECIAL CATEGORIES OF PERSONAL DATA

- Racial or Ethnic Origin
- Political Opinions
- Religious or Philosophical Beliefs
- Trade Union Membership
- Sex Life or Sexual Orientation
- Genetics
- Biometrics (e.g. Fingerprints, Residence Permit, Passport)
- Health Records

CRIMINAL RECORDS DATA

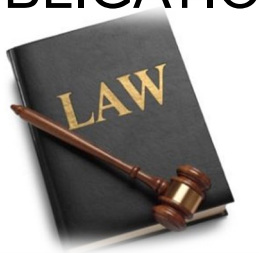
Criminal records data is extremely sensitive personal data that can be handled in specific and limited circumstances

GDPR: LAWFUL BASIS FOR PROCESSING DATA

UCL

CONSENT

LEGAL OBLIGATION



PUBLIC INTEREST

CONTRACT

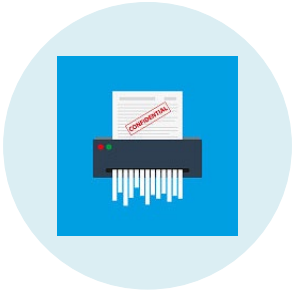
VITAL INTEREST

LEGITIMATE INTEREST

GDPR: KEY PRINCIPLES

Be transparent with data

Must ask for consent



Limit data to what you need

Only ask for what you need

Data must be accurate

Make sure data is accurate and complete

Limit storage of personal data

Don't retain for longer than necessary

Integrity and confidentiality

Keep your data safe

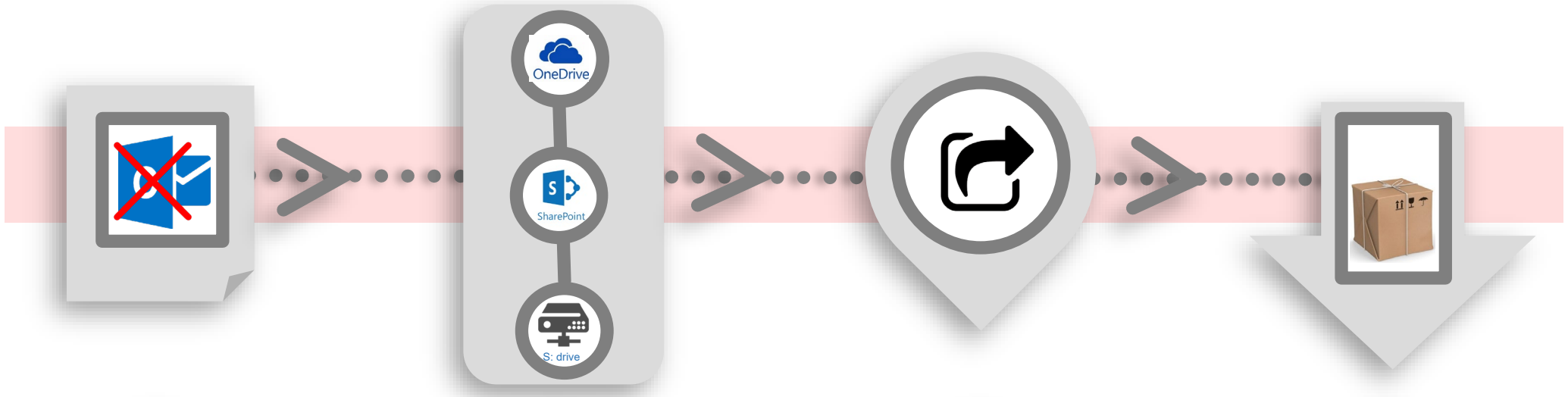
Accountability

Keep a paper trail to document compliance

Drop + Collect

Do you need to transfer personal data?

Here's how it's done.



1

PERSONAL DATA

Need to transfer personal data

2

STORE SECURELY

Leave for collection

3

SHARE LINK

Share link with recipient

4

COLLECT

Recipient collects from secure location

DATA BREACHES

We are all human and mistakes happen

When personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data without authorisation.

Are any cases where personal data is almost lost.

Err on the side of caution

REPORTING AN INCIDENT

Immediately report incidents to the UCL Information Security Group:

Fill in the **Personal Data Breach Form** then email it to us:
Email: isg@ucl.ac.uk
Telephone: (0)20 7679 7338 (internal 37338)

Do NOT report incidents externally, e.g. to the ICO or press.

Scenario 1: Disciplinary Investigation

The Head of the department has contacted you and has raised concerns about inappropriate behaviour from their direct report. They would like you to investigate whether formal disciplinary action should be taken. So far, you have gathered information about the case mainly via email; you decide to contact the Head of Department's PA to arrange a meeting to discuss the matter.

Activity

While undergoing your investigation, what will you need to consider in your day-to-day practices to ensure that the personal data is kept safe?

Answer

- The transfer of data should be a ‘drop and collect’ transfer, rather than email.
- Store the data in a UCL managed storage device (S drive, OneDrive, SharePoint).
- Documents should be shared via hyperlink to their location and not via email. Access should be given only to relevant people.
- Any handwritten documentation should be either scanned and saved in a suitable area and paper copies shredded (Ensure the digital copy first!) or stored in a lockable cabinet in a lockable office.
- The PA doesn’t need to know the details of the individual case.
- De-personalise emails, calendar entries, etc.
- Ensure that the room booked for the meeting is appropriate, e.g. not open plan, café, etc.
- Ensure that when you book a room to make the event ‘private’ and not to include files in the invite.

Scenario 2: Budgets

You are working on a research project, and you are submitting a grant application to a funder. The funder has asked that the grant application includes details of each person who will work on the research including their name, surname, position at the University, Tax and NI details, as well as their remuneration.

Activity

The PI has asked you to compile the information as requested and send it to the funder. How would you go about securing this information and transferring it to the funder?

Answer

- Query why such information is being requested and don't be afraid to say no if the funder cannot establish a lawful reason for requesting Tax and NI details.
- Some major funders use secure portals to upload documents; if this is not available, The transfer of data should be a 'drop and collect' transfer, rather than email.
- Store the data in a UCL managed storage device (S drive, OneDrive, SharePoint).
- Documents should be shared via hyperlink to their location and not via email. Access should be given only to relevant people.

Scenario 3: A newsletter

Your department has decided to begin issuing a fortnightly newsletter to people who sign up for one. You have established a website where people can register their interest in the newsletter and are preparing to publish it. A member of senior management informs you that they have a list of c. 100 peoples contact details who would be interested in receiving the newsletter, please add them to the contact list and include them in the publication

Activity

a)What are the data protection considerations in this scenario?

b)What tools can you use to ensure that you meet the principles of the data protection legislation

Answer

- Review and follow the guidance note here: https://www.ucl.ac.uk/legal-services/ucl-general-data-protection-regulation-gdpr/guidance-notices-ucl-staff/guidance-note-actions-take
- If you choose to go ahead with these contacts, you must develop a privacy notice, and ensure there is an unsubscribe function in the communication.

Support and Advice

Your first ‘port of call’ should always be the UCL GDPR website – www.ucl.ac.uk/gdpr.

- Programme information
- FAQs
- Updates to legislation
- Webinars
- Guidance

You may contact the programme using GDPR@ucl.ac.uk

Training: www.ucl.ac.uk/gdpr-online-training