Information security

Data classification

<P15.OU106 Strengthening Identity & Access Management>

London Metropolitan University

Information and Technology Services

Programme Management Office

Author: Elaine Dimon
Version: 2.0
Date: 19 December 2016
+44 (0)20 7133 2407
e.dimon@londonmet.ac.uk

Contents

Change history

Date	Version	Amended by	Change/update
04.10.2016	0.1	Elaine Dimon	Initial draft
10.10.2016	0.2	Elaine Dimon	Added Data protection reform Added Network management Added links for: - GDPR Regulations (EU Council Directive) - Information Protection (Security) Policy Minor changes to wording Added reference section
14.10.2016	0.3	Elaine Dimon	Edited Purpose section Removed references to interfaces and network management and added note to Scope section Added NDA as pre-requisite for Confidential and Restricted data Added Glossary Moved links & references to the end
02.11.2016	0.4	Elaine Dimon	Changes from review with Peter Garrod and Tracy Brathwaite 28.10.2016 Added **Internal** category
07.11.2016	0.5	Elaine Dimon	Handling & storage matrix - minor clarifications from review by Hemanth Shanthigrama
24.11.2016	1.0	Elaine Dimon	Minor changes to Internal and Public examples as advised by Peter Garrod - baseline document v1.0
19.12.2016	2.0	Elaine Dimon	Minor changes as advised by Raghu Vydyanath

Glossary

Term/Acronym	Meaning
Affiliates	Individuals who are not payroll employees or students of the University. They do not have a presence in SAP or SITS. Accounts for affiliates should be managed using the ARMS system. MET Temps are treated not affiliates
ARMS	Affiliates Record Management System
SAP	Systems, Applications & Products in Data Processing - University HR system
SITS	Strategic Information Technology Services - Student records system
SIAM	Strengthening Identity and Access Management
GDPR	General Data Protection Regulation

Introduction

There are a number of different applications and systems used by London Metropolitan staff, students and affiliates which contain varying degrees of personal and commercially sensitive information. In order to maintain the appropriate levels of confidentiality (the wrong people obtaining information), integrity (information being altered deliberately or accidentally without permission) and availability (information not being available when it is required) of the data held, they must be protected against any unauthorised access, modification or disclosure.

The security measures that should be applied depend on the sensitivity of the data and relate to all types of information, not just that which is covered by the Data Protection Act (DPA) and the EU General Data Protection Regulation (GDPR).

Purpose

To document, define and agree the classification levels to use in the SIAM project for assessment of authentication required for applications.

The classification levels defined are appropriate for all of the University's information assets (documents, reports, presentations, emails, intranet content and any other data held by the University) for use in a future universal 'Data Classification' policy. As such, the definitions are written in a format that could be reused for that purpose. They are in alignment with the commitments to data security in the University's Information Protection (Security) Policy which states that "The widest possible definition of security will be used to include all types of incident that impact the effective use of information. This includes performance, consistency, reliability, confidentiality, integrity and availability".

Scope

Data stored on computers and portable devices, printed out or written on paper, sent by fax, stored on tapes, disks or electronic appliances, or spoken in conversations and over the telephone are included in this proposal and it applies to anyone using the University's information systems.

Exchange or storage mechanisms and other forms of information management including, but not limited to, interfaces and network management will require further consideration and are out of scope for this document.

Any specific legal or contractual clauses relating to the classification of information should override the conventions set out in this document.

EU data protection reform

The General Data Protection Regulation (GDPR) was due to be implemented in the UK in May 2018 to replace the existing Data Protection Act. Although the result of the EU referendum in June 2016 may have some impact, the principles and concepts will still be relevant to the University and the GDPR will be able to impose increased compliance regulations and increased fines for non-compliance.

The GDPR definitions for 'Personal Data' and 'Sensitive Personal Data' are generally the same, but there are some additional regulations to account for the way that changes in technology are used to collect information about people. Personal data where a key is used for identification, such as a student ID, can fall within the scope of the GDPR depending on how difficult it is to attribute the key to a particular individual. This type of association also applies to identifiers such as IP addresses where individuals may be recognised from other information obtained by the servers.

> *(1) 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural 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, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;*
>
> (Council Directive 2016/679 art.4)

Key points

- Information should be classified at one of four levels: **Confidential, Restricted, Internal** and **Public**.

- In addition to the sensitivity of the data, the classification should also take into consideration the criticality to the University in respect of reputation, value and the number of individuals potentially affected by a breach.

- Where there are collections of data that range in sensitivity, the most restrictive classification of any of the individual data elements should be applied.

- If there are any changes made to the value, sensitivity and criticality of the information held, the classification should be reviewed and updated accordingly as necessary. This is an important consideration even if the level of sensitivity or criticality has reduced, e.g. after a period of time the information has become public, because over-classification can result in extra expense maintaining controls that are not required.

Information Owners

All areas where data is stored by the University should have an associated Information Owner. It is the responsibility of the Information Owner to assess and classify the sensitivity of the data and to ensure that appropriate controls are applied accordingly.

Policy breaches

For information regarding breaches relating to this policy, please refer to the DP data breach incident reporting document.

Data classification policy

The following details provide an outline of the four categories to be used for the classification of sensitive information. Staff, students, third-party agents and affiliates of the University receiving sensitive information in any format are required to manage that information in accordance with this policy to protect it from disclosure to unauthorised recipients.

A. Confidential

Where unauthorised disclosure or distribution could result in severe financial or reputational damage and has considerable value to the University, data should be classified as '**Confidential**'.

Information that is defined by the Data Protection Act (DPA) as 'Sensitive Personal Data' should be included in this category. It should not be shared with third parties unless there is an NDA (Non-disclosure agreement) in place.

Access should be restricted to those who specifically need it to perform their duties and it should be controlled at levels according to what is necessary do their job. Confidential data held outside the University (on mobile or storage devices including laptops, phones, tablets, USB sticks etc.) – must be protected behind an explicit logon and by Advanced Encryption Standard (AES) encryption.

Examples of Confidential data:

1. DPA defined 'Sensitive Personal Data' relating to:
    a. The racial or ethnic origin of an individual
    b. Political opinions
    c. Religious beliefs (or other beliefs of a similar nature)
    d. Membership of a trade union
    e. Physical or mental health
    f. Sexual orientation
    g. The commission or alleged commission of any offence
    h. Any proceedings for any offence committed or alleged to have been committed

2. Salary details

3. Bank details

4. Passwords

5. Contract negotiations

6. Information that is subject to a confidentiality agreement

7. Data where serious breach has a potential for ID theft, could result in local or national media coverage or affects more than 1000 people

B. Restricted

Where disclosure or distribution could incur some negative publicity, but is not likely to cause severe financial or reputational damage to the University, data should be classified as '**Restricted**'.

Information that is defined by the Data Protection Act (DPA) as 'Personal Data' should be included in this category. It should not be shared with third parties unless there is an NDA (Non-disclosure agreement) in place.

Access should be subject to controls with valid logons for specified groups of staff. Restricted data held outside the University (on mobile or storage devices including laptops, phones, tablets, USB sticks etc.) – must be protected behind an explicit logon and by Advanced Encryption Standard (AES) encryption.

Examples of Restricted data:

1. DPA defined 'Personal Data'. Relating to an individual:
    a. Address (home or work)
    b. Age
    c. Telephone number
    d. Educational institutions attended
    e. Photographs
    f. Emergency contact, next of kin details

2. Information held under licence

3. Paperwork from statutory and other formal committees

4. Commercially sensitive communications

5. Plans, strategies and projections

6. Management information (MI)

7. Data where serious breach could cause damage to a department or service's reputation, could result in low key or HE media coverage or involves sensitive data such as redundancies and restructuring for 20 -100 people

8. Lecture materials that include information subject to copyright

C. Internal

Where information should be available to authenticated members of the University, disclosure or distribution is not likely to generate negative publicity, cause severe financial or reputational damage, data should be classified as '**Internal**'. This data is not intended for distribution outside the University, although in some cases it may be released later with possible restrictions on content and/or time of publication.

Access should be subject to controls with valid logons for all staff and students. Information classified as **Internal** may be restricted to specific subsets of University members e.g. Students should not have access to data stored in the 'Staff Zone'.

Examples of Internal data:

1. Internal only University policies, processes and guidelines
2. Internal only job advertisements
3. Internal staff communications
4. Information that may be intended for public release at a later date
5. Lecture materials that do not include information subject to copyright
6. Surveys

C. Public

Information that is available to the general public and is intended for distribution outside the University or where disclosure and distribution would have no significant reflection on any individual or body and would be unlikely to attract media interest can be classified as '**Public**'. It can be disclosed and distributed with no restrictions on content, audience or time of publication, providing that it does not violate any applicable laws or regulations e.g. privacy.

No controls are placed on general read-only access, but modification should be restricted to individuals that have been approved by the Information Owners. Access for modification should be controlled with appropriate authentication.

Paper based information can be kept in unsecured storage.

Examples of Public data:

1. Annual accounts
2. Public website information
3. News releases
4. Job advertisements/ roles/ grades (excluding internal only positions)
5. Salary bands
6. Course information
7. Unrestricted strategies, policies and procedures

Desks and screens

Paper based information that has been classified as **Confidential** or **Restricted** should be kept in locked storage.

Workspaces must be cleared of documents with classification **Confidential** or **Restricted** when they are away from their desks for an extended period of time and at the end of each working day.

Users should lock their computer screens if they are away from their desk for more than 3 minutes and log out or switch off at the end of each working day.

Disposal of media

Media should be disposed of in a manner so that any information it contained is unable to be recovered.

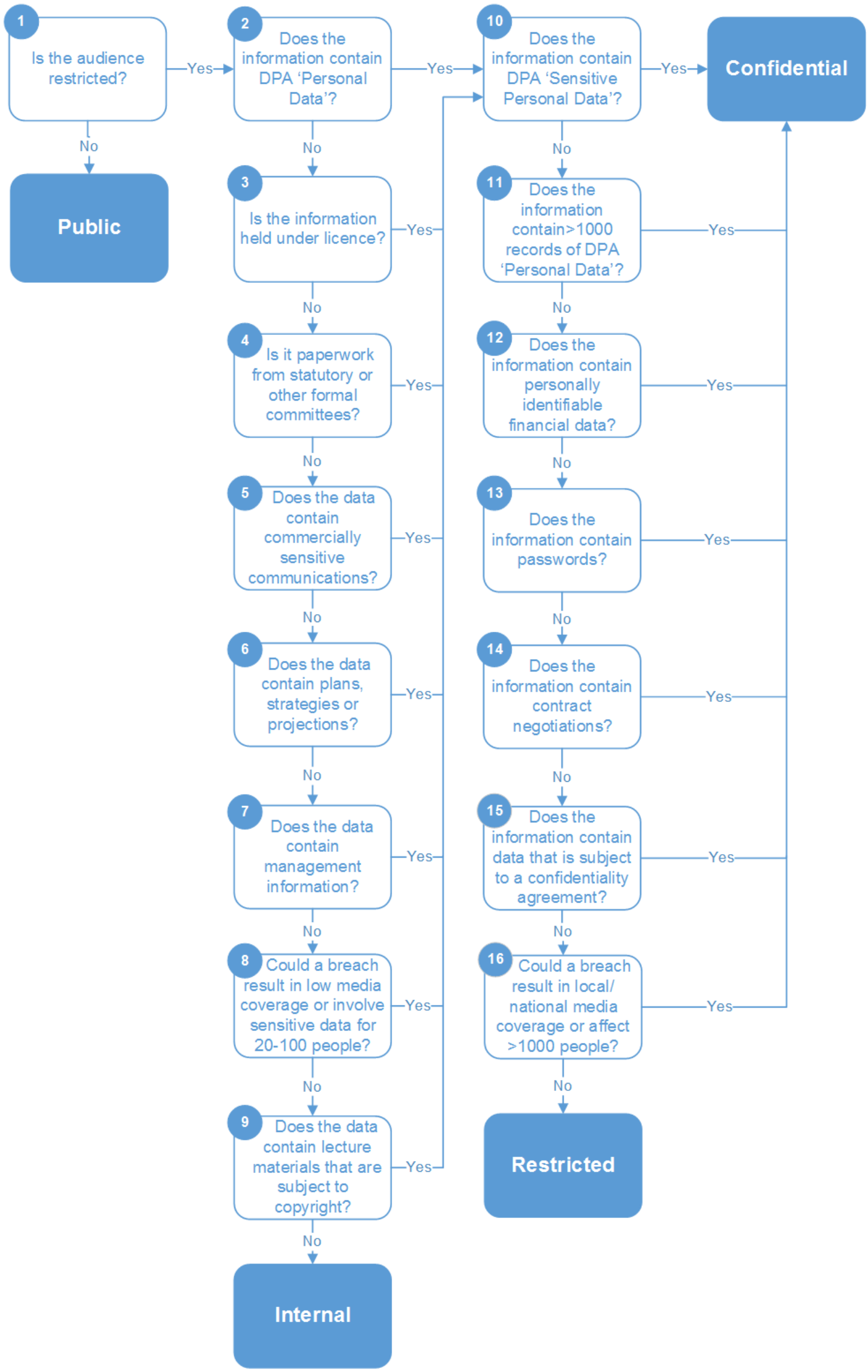
Please refer to the ITS document: *Disposal of ICT Assets*.

Handling & storage matrix

Classification	Examples	Access control	Storing on paper	Storing digitally	Sharing on paper	Sharing digitally
Confidential	- DPA defined 'Sensitive Personal Data' relating to: - The racial or ethnic origin of an individual - Political opinions - Religious beliefs (or other beliefs of a similar nature) - Membership of a trade union - Physical or mental health - Sexual orientation - The commission or alleged commission of any offence - Any proceedings for any offence committed or alleged to have been committed - Salary information - Bank details - Passwords - Contract negotiations - Information that is subject to a confidentiality agreement - Data where serious breach has a potential for ID theft, could result in local or national media coverage or affects more than 1000 people	Controlled at levels according to what is necessary do a specific job Strict need-to-know basis	Kept in locked storage when not in use Keep out of sight when not immediate focus of work Do not take offsite if possible (If necessary store in sealed or locked bags, drawers or rooms. Return to office for secure destruction)	Only on University owned devices Store on X: drives or other restricted areas – check who can access them User ID & Password Offsite – Only on encrypted devices. Sealed or locked drawers, bags or rooms. Stored out of sight. Password required. Delete as soon as possible	Hand-deliver documents Non-disclosure agreement with third party Use a secure courier	Start email subject with "Confidential" Encrypted email where possible Non-disclosure agreement with third party is a prerequisite Use individual share options on Google Drive in a separate folder
Restricted	- DPA defined 'Personal Data'. Relating to an individual: - Address (home or work) - Age - Telephone number - Educational institutions attended - Photographs - Emergency contact, next of kin details - Information held under licence - Paperwork from statutory and other formal committees - Commercially sensitive communications - Plans, strategies and projections - Management information (MI) - Data where serious breach could cause damage to a department or service's reputation, could result in low key or HE media coverage or involves sensitive data such as redundancies and restructuring for 20 -100 people - Lecture materials that include information subject to copyright	Subject to controls with valid logons for specified groups of staff or students Need-to-know basis	Kept in locked storage when not in use Keep out of sight when not immediate focus of work Do not take offsite if possible (If necessary store in sealed or locked bags, drawers or rooms. Return to office for secure destruction)	Only on company owned devices and authorised personal devices e.g. smartphones and tablets with an explicit logon Store on X: drives or other restricted areas – check who can access them User ID & Password Offsite – Only on encrypted devices. Sealed or locked drawers, bags or rooms. Stored out of sight. Password required. Delete as soon as possible	Use internal mail or hand-deliver Use a secure courier	Encrypted email where possible Non-disclosure agreement is a prerequisite If sharing externally confirm with Information Owner
Internal	- Internal only University policies, processes and guidelines - Internal only job advertisements - Internal staff communications - Information that may be intended for public release at a later date - Lecture materials that do not include information subject to copyright	Subject to controls with valid logons for all staff and students May be restricted to specific subsets of staff and/or students	Can be stored/left on desks in secured areas Do not take offsite if possible	Only on company owned devices and authorised personal devices e.g. smartphones and tablets	Use internal mail or hand-deliver	If sharing internally – ensure that the data can be only be accessed by authorised University members or those who it is intended for If sharing externally confirm with Information Owner
Public	- Annual accounts - Public website information - News releases - Job advertisements/ roles/ grades (excluding internal only positions) - Salary bands - Course information - Unrestricted strategies, policies and procedures	Access for modification should be controlled with appropriate authentication	N/A	N/A	No constraints	No constraints

Quick check

Important note: If you are not sure about any of the questions, progress to the next most restrictive classification in the flow or check with someone who knows.



References

Council Directive 2016/679/EC of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).