LONDON’S GLOBAL UNIVERSITY

UCL

HANDLING PERSONAL DATA: YOUR RESPONSIBILITIES

UCL GENERAL DATA PROTECTION REGULATION (GDPR) PROGRAMME

CONTENTS

HANDLING PERSONAL DATA: YOUR RESPONSIBILITIES

The General Data Protection Regulation (GDPR) and the Data Protection Act (DPA) 2018 took effect on 25 May 2018 and have direct effect on EU member states resulting in a new, consistent set of data protection requirements. The data protection legislation gives people the right to know what information is held about them, and requires the University to ensure that personal information relating to living individuals is handled according to a set of seven principles.

The data protection legislation is a complete overhaul of the Data Protection Act (DPA) 1998 and it has been developed to strengthen personal data protection and online privacy rights and is the same across all EU member states. It is the most significant change to data protection law in 20 years.

Why now? Since 1995 new technologies - mobile devices, social media and pervasive use of the internet - have fundamentally changed the way we use personal data and shown the current DPA to be inadequate in terms of protection of personal data.

The data protection principles are as follows:

a)	data must be processed lawfully, fairly and in a transparent manner in relation to individuals ('lawfulness, fairness and transparency');
b)	data is collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes ('purpose limitation');
c)	data is adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');
d)	data is accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which it is processed, is erased or rectified without delay ('accuracy');
e)	data is kept in a form which permits identification of data subjects for no longer than is necessary and for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals ('storage limitation');
f)	data is processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality') and
g)	the controller shall be responsible for, and be able to demonstrate compliance, with a – f above (accountability)

GDPR APPLIES TO INFORMATION RELATING TO PEOPLE

PERSONAL DATA

The GDPR applies to ‘personal data’ meaning any information relating to an identified or identifiable living person.

This definition means a wide range of personal identifiers would constitute personal data, including name, identification number, location data or online identities. This reflects changes in technology and the way organisations collect information about people.

The GDPR applies to both personal data held electronically and in manual filing systems. This could include chronologically ordered sets of manual records containing personal data and email.

Personal data that has been pseudonymised – eg key-coded – falls within the scope of the GDPR.

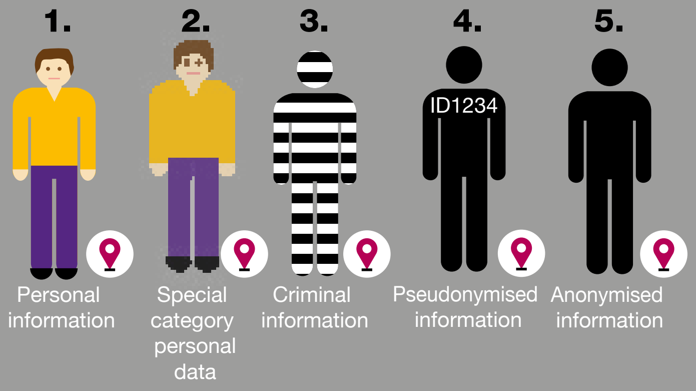
SENSITIVE PERSONAL DATA

The GDPR refers to sensitive personal data as “special categories of personal data” and is data that is seen as being particularly sensitive and that needs to be processed by organisations with extra care and attention.

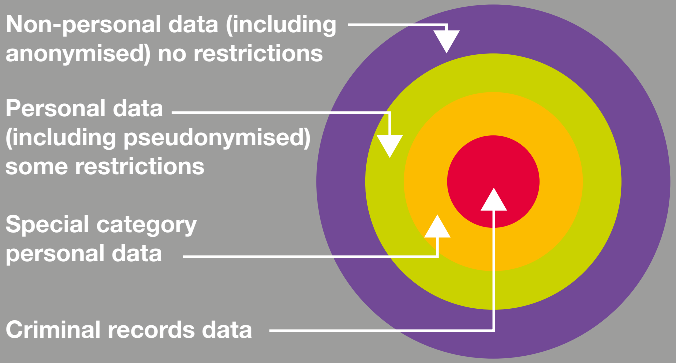
The special categories specifically include health, trade union membership, ethnic origin, religious / philosophical belief, sexual orientation, genetic data, and biometric data where processed to uniquely identify an individual.

Personal data relating to criminal convictions and offences are not included, but similar extra safeguards apply to its processing.

DATA TYPES



AND THERE ARE LEVELS OF DATA SENSITIVITY


Non-personal data (including anonymised) no restrictions
Personal data (including pseudonymised) some restrictions
Special category personal data
Criminal records data

DATA TYPES

Consent
Explicit consent requires a clear and specific statement of consent, including a reason for collection

Transparency
Be clear on how data will be collected, used and stored

Data portability
Individuals can obtain and reuse their personal data for their own purposes across different services

Erasure
Individuals have the right to remove personal data if there is no compelling reason for storing it

Correction
Personal data must be changed if it is incorrect or incomplete

Automated process
Individuals have rights not to be subject to a decision based solely on automated processing, including profiling.

UCL'S RESPONSIBILITY

Accountability
Controllers must demonstrate compliance with the GDPR principles: lawful, fair, transparent, purpose limitation, data minimisation, accuracy, storage limitation integrity and confidentiality

Data breaches
When a personal data breach occurs, that there are procedures in place to identify and report the breach to a competent supervisory authority within 72 hours

Data Privacy Impact Assessment (DPIA)
Identify, assess and mitigate or minimise privacy risks with data processing activities

Data security
Adequate technical, policy and procedures to protect personal data and systems must be in place. ‘Privacy-by-design’ to be considered at the start of development of systems and products, not at the end

Data transfer
To be governed by tough GDPR rules and includes non-EU countries that process personal data of individuals in the EU

Data Protection Officer (DPO)
Appointed to take responsibility of data protection compliance

THE RISK OF NON-COMPLIANCE – POWERS AND FINES

Fine
If found non-compliant the ICO can implement fines of €20m or 4% of annual turnover, whichever is greater

Compensation
Individuals will have the right to claim compensation for any damage suffered as a result of contravening the GDPR if it is proven to cause harm to them

Reputation
The impact on the organisation is not just financial, partners may not want to do business and trust could be impacted

CONTENTS ◀ ▶

1. INTRODUCTION TO THE GDPR PREPAREDNESS PROGRAMME

On 25 May 2018, the EU General Data Protection Regulation (GDPR) comes into force across the European Union (EU).This legislation introduces sweeping changes to the way in which personal data can be collected, used, retained and deleted. Furthermore, it significantly increases the penalties for non-compliance – 20million Euros or four percent of worldwide turnover.

Essentially GDPR is about accountability and transparency; being clear with people about how their data is used and putting high standards of data protection at the centre of how we do business.

To meet the challenge of compliance posed by GDPR, UCL has established a GDPR Programme that will provide strategic planning and action change.

The GDPR Programme is broken down into two phases to make it more manageable and to accelerate delivery where possible.

The two phases will be:

Phase 1 - Investigation, emphasises an evidence-based approach to inform decision-making, such as prioritising high-risk areas then recommending controls to mitigate risk. Phase 1 has four workstreams: Non-Research Data, Research Data, Training and Policy & Process and will be completed by December 2018

Phase 2 - Implementation, puts in place the recommendations made in Phase 1 and monitors compliance progress, this phase will commence after December 2018

This briefing booklet sets out the work that will be taking place until December 2018 as part of Phase 1 – Investigation.

2. GDPR PROGRAMME GOVERNANCE

The UCL GDPR Programme is ultimately governed by the UCL Senior Management Team (SMT), with responsibility delegated to the Strategic Programme Board (SPB), chaired by Professor Graham Hart (Dean, Faculty of Population Health Sciences and Senior Responsible Officer SIRO). Operational governance of the programme has been allocated to the GDPR Operations Board (OB), chaired by Wendy Appleby (Registrar, and Project Executive).

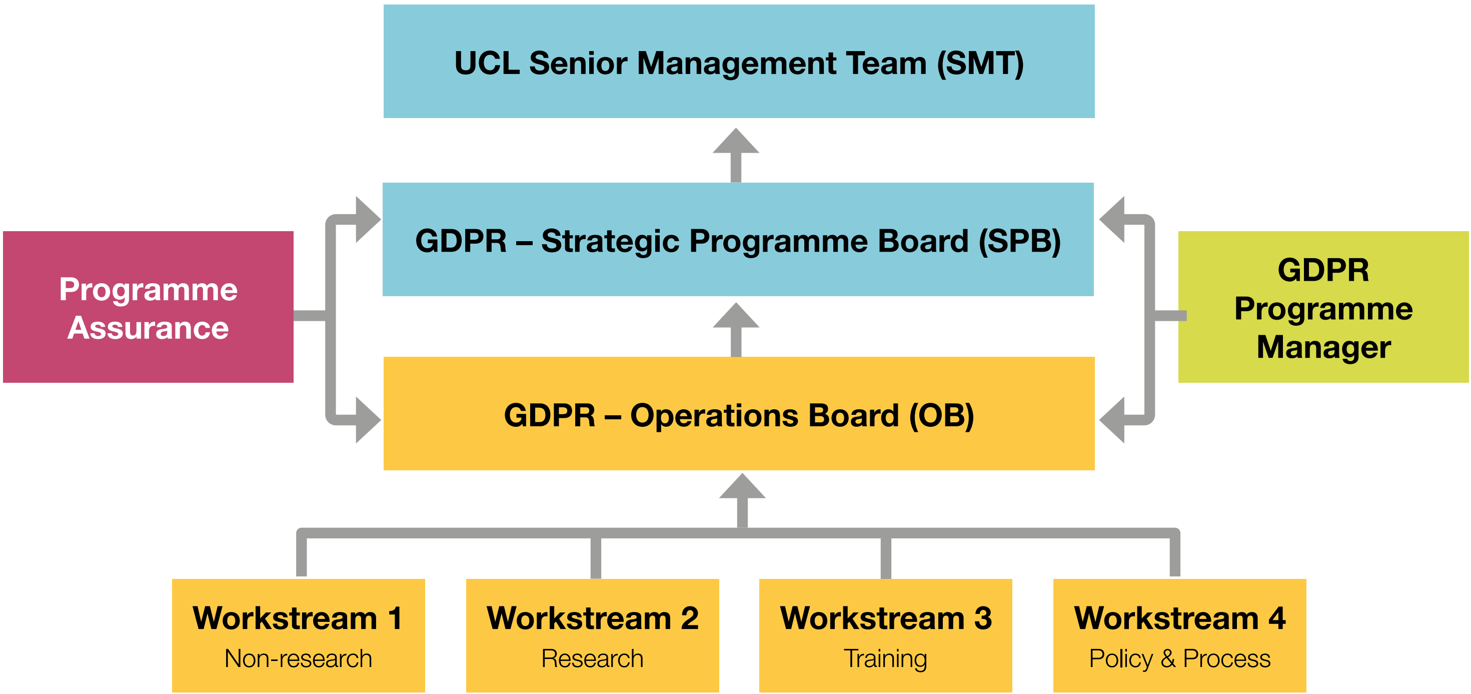
Phase 1 Delivery Team

Phase 1 of the GDPR Programme will be carried out by a core delivery team managed by Thibault Williams (GDPR Programme Manager). Thibault is supported operationally by three Project Managers for each of the workstreams (see below).

The Programme Assurance is responsible for ensuring Programme Governance is adhered to, and risk analysis and responses are adequately understood and managed, as well as providing financial assurance to the SPB. The Programme Assurance team are independent of the Programme, but the function will report, as required, to the SPB on matters which the Programme Assurance team deem appropriate to escalate to the SPB.

Key Suppliers of Services

Supporting the delivery team are a set of key suppliers, including a legal partner, the UCL Data Protection Officer (DPO), the Information Security Group (ISG), and the Information Services Division (ISD).



UCL Senior Management Team (SMT)

GDPR – Strategic Programme Board (SPB)

Programme Assurance

GDPR Programme Manager

GDPR – Operations Board (OB)

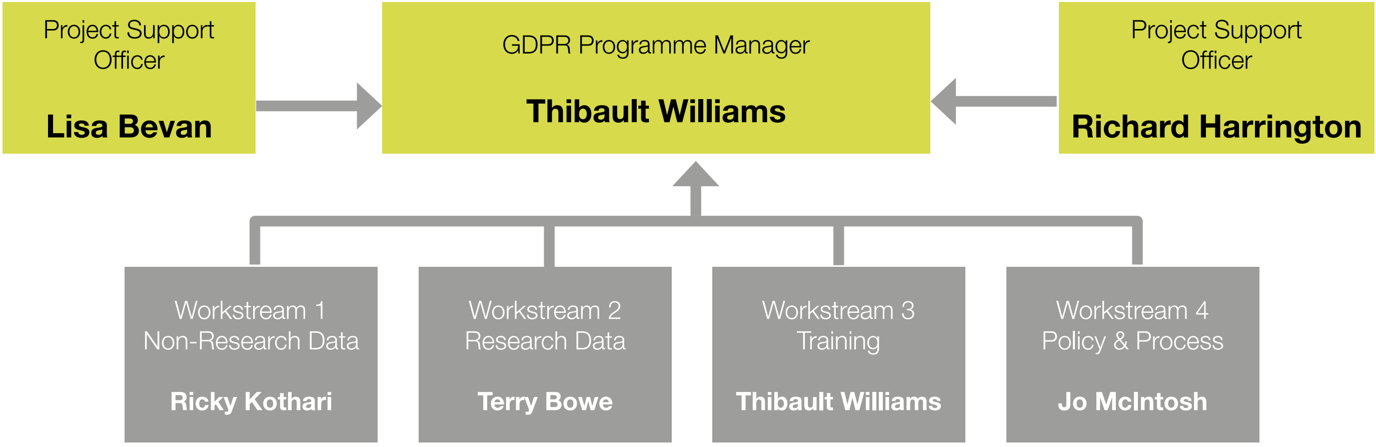
Workstream 1
Non-research

Workstream 2
Research

Workstream 3
Training

Workstream 4
Policy & Process

For Phase 1 – Investigation Stage



Project Support Officer
Lisa Bevan

GDPR Programme Manager
Thibault Williams

Project Support Officer
Richard Harrington

Workstream 1
Non-Research Data
Ricky Kothari

Workstream 2
Research Data
Terry Bowe

Workstream 3
Training
Thibault Williams

Workstream 4
Policy & Process
Jo McIntosh

3. GDPR PROGRAMME INVESTIGATION PHASE - WORKSTREAM OBJECTIVES

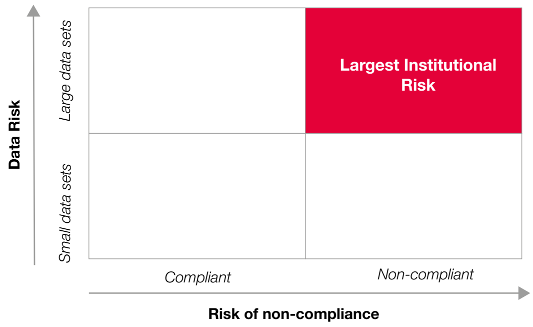
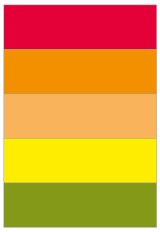
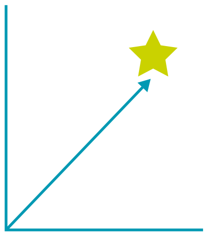
Objectives – Phase 1 – Investigation Stage

	WORKSTREAM 1 Non-research data	**WORKSTREAM 2** Research data
Objectives	Build an evidence-based approach that develops: • A robust understanding of non-research data holdings. • A clear understanding of non-research data GDPR compliance and institutional risk. • A clear understanding of compliance activity to prioritise and an understanding of capabilities required to carry out activity. • Logical plans to redesign non-compliant activity, upscale leading practice and embed data leadership. • A clear plan of action to inform Phase 2 implementation.	Build an evidence-based approach that develops: • A robust understanding of research data holdings. • A clear understanding of research data GDPR compliance and institutional risk. • A clear understanding of compliance activity to prioritise and an understanding of capabilities required to carry out activity. • Logical plans to redesign non-compliant activity, upscale leading practice and embed data leadership. • A clear plan of action to inform Phase 2 implementation.

	WORKSTREAM 3 Training	**WORKSTREAM 4** Policy & Process
Objectives	Create a well thought out training regimen that: • Is specific to UCL. • Covers both data protection and information security. • Is functional, usable, and has the capability to track users and completion rates. • Ensures high completion rates. • Is designed, developed, launched and completed by UCL staff by October 2018. Supports workstreams 1 & 2 where required	Build a robust view of all UCL policies that concern or affect data protection, including: • A detailed understanding of central policies and processes. • A detailed understanding of departmental policies and processes. • Embedding data protection into future creation of policies and processes. Supports workstreams 1 & 2 where required

Outcome	• A reduction in the risk of UCL being non-compliant with GDPR and the associated financial, and reputational risk. • Improved business processes. • Reduction in the future data storage requirements. • Reduction in overheads related to data collection, and retention. • Improved business awareness of data protection matters.

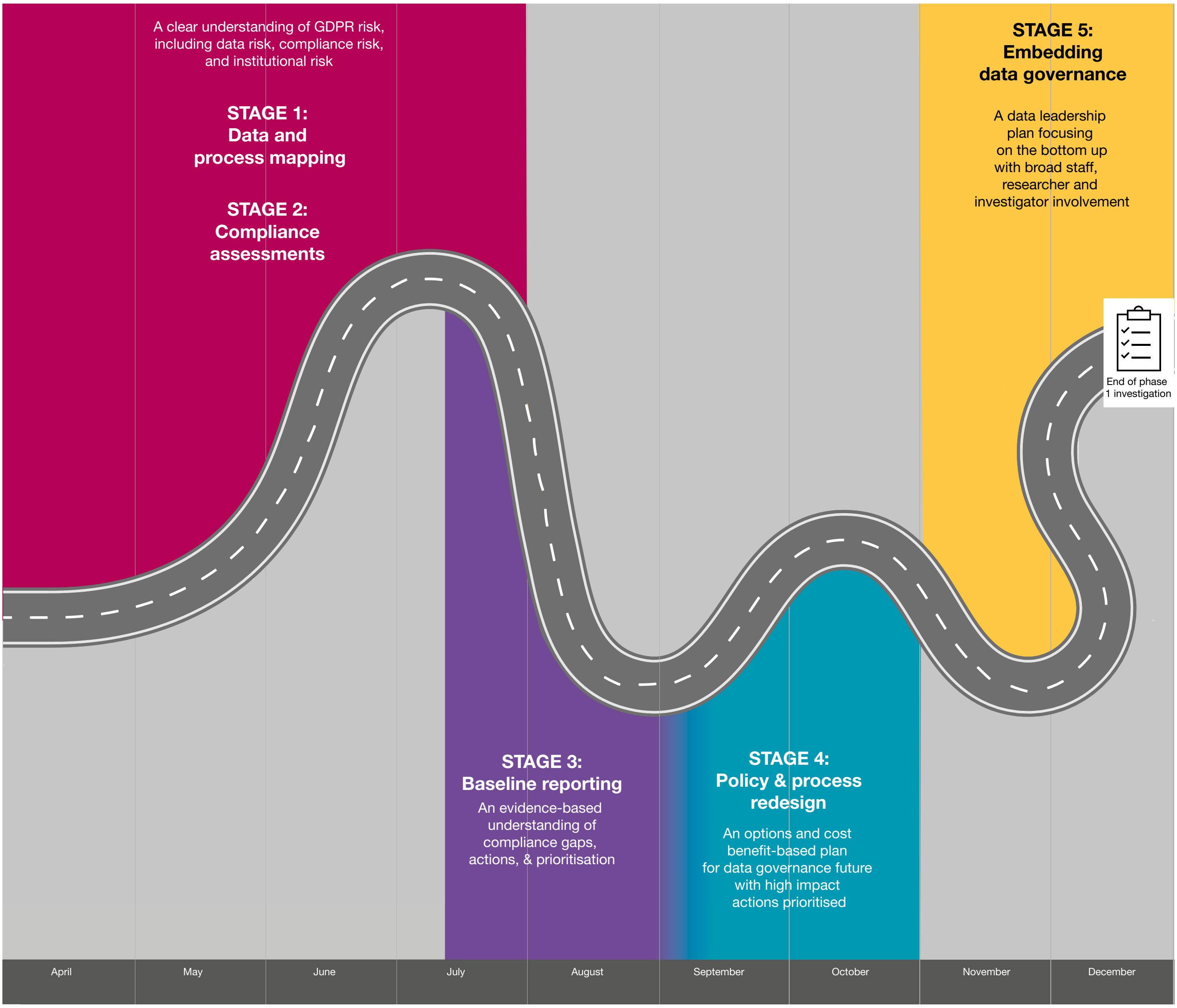
4. GDPR PROGRAMME INVESTIGATION PHASE - APPROACH

STAGE	1. Data & Process Mapping	2. Compliance Assessment	3. Baseline Report	4. Policy & Process Redesign	5. Embedding Data Governance /Leadership
	 Data Risk Large data sets Small data sets Largest Institutional Risk Compliant Non-compliant Risk of non-compliance				
OUTPUT/ OUTCOME	A clear understanding of GDPR risk, including data risk, compliance risk, and institutional risk		An understanding of compliance gaps, required actions & prioritisation	A capability and cost benefit-based plan for the data governance future with high impact actions prioritised	A data leadership plan with broad staff, researcher and investigator involvement

GDPR Programme Phase 1 Investigation Approach Detail

Stage	Title	Description	Deliverables
1	**Data and process mapping**	Includes a 'personal' and 'special category personal data' mapping exercise to define where research and non-research data is stored, its age, how it is collected and how it is processed, together with an assessment of existing security policies, practices and processes.	• GDPR Information Architecture Map • GDPR Central Information Asset Register
2	**Compliance Assessment**	The compliance assessment is a survey-based tool developed with support of our legal partners to assess compliance to GDPR. The survey will be rolled out across Professional Services and Research Departments.	• GDPR Compliance Assessment
3	**Baseline Reporting**	Baseline reporting will incorporate outputs from stages 1&2 to report the 'current state' of compliance as well as 'direction of travel'. A RAG rating will be applied to faculties and departments, and across faculties and departments to highlight key risk areas.	• GDPR Baseline Report
4	**Policy & Process Redesign**	Following the baseline report, policies and processes will be redesigned to improve compliance within identified 'risk areas'. This will include a revision of consent policies and processes where necessary. At the same time, capabilities will be assessed to understand the cost/ benefit of defined actions.	• GDPR Policy & Process Redesign Plan • Capability Assessment
5	**Embedding Data Leadership**	To oversee compliance and data management improvements, governance processes will be amended to establish and embed new ways of working with personal data across the UCL. Training will also be delivered at this stage.	• GDPR Staff Training
6	**Project Closure**	At the closure of all the workstreams; project closure, project finance and lessons learned reports will be provided together with a high-level implementation plan for use in kicking off Phase 2.	• GDPR High-level Implementation Plan • Closure Report

5. GDPR INVESTIGATION PHASE - ROADMAP TO COMPLIANCE



A clear understanding of GDPR risk, including data risk, compliance risk, and institutional risk

STAGE 1: Data and process mapping

STAGE 2: Compliance assessments

STAGE 3: Baseline reporting

An evidence-based understanding of compliance gaps, actions, & prioritisation

STAGE 4: Policy & process redesign

An options and cost benefit-based plan for data governance future with high impact actions prioritised

STAGE 5: Embedding data governance

A data leadership plan focusing on the bottom up with broad staff, researcher and investigator involvement

End of phase 1 investigation

6. WHAT YOU CAN DO NOW

FAMILIARISE YOURSELF WITH THE GDPR

There is a very large amount of information available online and in the news. All staff are encouraged to visit the following websites to seek further information and details about GDPR:

- **The ICO website (https://ico.org.uk) has guidance on:**

  Consent https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/consent/

  Legal basis for processing https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/

  Transparency and privacy notices https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-notices-transparency-and-control/

  Retention https://ico.org.uk/for-organisations/guide-to-data-protection/principle-5-retention/
- **EUGDPR.org – https://eugdpr.org.uk**

UNDERTAKE CURRENT TRAINING:

Take the current DPA and Information Security Training which is available on UCL Moodle - https://www.ucl.ac.uk/legal-services/training

IF IN DOUBT, SHOUT! – If you require assistance with your storage solution contact your departmental IT representative

CHECK THE FOLLOWING ITEMS FOR ALL CURRENT/HISTORICAL PROJECTS WHERE PERSONAL DATA WAS COLLECTED

- Do you process personal data?
- Do you retain personal data?
- Do you have any processes that need reviewing?
- Review the current UCL Data Retention Schedule (https://www.ucl.ac.uk/library/docs/retention-schedule.pdf) to ensure you are keeping data within the specific retention periods.

If you find that you have been storing data beyond the retention date do not panic. Undertake the following checklist:

  - Where is the data stored? If this is not on a UCL managed service (UCL S: Drive, UCL SharePoint, UCL One Drive, or any other UCL owned and managed storage), please contact your IT representative to make arrangements to move this data to UCL managed services.
  - Document what data is stored and where it is stored on UCL managed services, when the data was collected, by whom and who the owner of the data is now. If these details are not known, take a decision within your department to assign a data owner.
  - Ensure that access to this data is restricted to only those persons who require the data.
  - Do not delete the data from the UCL managed services. Later in 2018 the GDPR programme will issue new guidance and processes for the deletion of personal data on UCL managed services.
- When the GDPR assessments are conducted across the University, please note this transfer to the GDPR project team who will log this information and include this as part of the wider Programme.
- Store research data in the UCL Data Safe Haven (please note this is not for archiving).
- Discuss your data requirements with your IT representative and discuss the option of using UCL managed storage services. Do not store personal data on non-UCL managed services (e.g. Dropbox, Google Drive, Google shared document etc).
- Discuss with your IT representative the use of encryption tools such as 7Zip (available free from UCL software database: https://swdb.ucl.ac.uk/
- If your department is using the S:Drive ensure your folders are restricted using role account access, and if required, encrypted.
- Ensure that where you are using encryption and/or passwords, that these are not stored separately.

IF YOU NEED TO TRANSFER PERSONAL DATA:

1. Ask yourself: “why are you sending this personal data?” Could this data be sent without the personal details?
2. If you still need to send the personal data use one of the following options:

   1. E-mail: Encrypt the file using 7Zip. Contact the recipient to tell them the password. DO NOT DO THIS VIA E-MAIL (do not include the password in the email with the file).

   For internal UCL transfers:

   1. Create a shared folder on the S:Drive where you can save the file and grant the recipient access to the folder, and notify them when the file is ready for collection.
   2. If this is going to be regular task, create a SharePoint site (http://www.ucl.ac.uk/isd/services/comms-collaborate/sharepoint). Restrict access to folders to the recipient only. Upload your file to the folder and notify the recipient that the file is ready for collection.
   3. Upload your file to UCL Onedrive. Share the link to the file with the recipient.

   For external UCL transfers:

   1. Wherever possible use a secure web interface to transfer the data. Many regulatory bodies and/or companies have secure file transfer systems in place. Please discuss this with the receiving party.
   2. You may upload the file to UCL OneDrive and share the link with an external recipient. You should encrypt the file and share the password separately.

   If you need assistance - contact the UCL Service Desk servicedesk@ucl.ac.uk

DATA BREACH

Reporting a loss of personal data

Under the General Data Protection Regulation (GDPR) data controllers, such as UCL, have a responsibility to ensure that the personal data they are processing is done in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable, for example, when it has been encrypted by ransomware, or accidentally lost or destroyed.

In cases where there has been an incident which resulted in a potential breach of the GDPR, it is imperative that you report this immediately to Information Security Governance.

For more information and guidance on how to report a loss of data please visit the UCL Data Protection webpage: https://www.ucl.ac.uk/legal-services/guidance/reporting-loss-personal-data

CONTENTS ◀ ▶

7. CASE STUDY 1: MANAGING A RESOURCE POOL

Linked to the “lawfulness, fairness and transparency” principle in GDPR and how compliance with Articles 12-14 is achieved.

Article 12: “Transparent information, communication and modalities for the exercise of the rights of the data subject”
Article 13: “Information to be provided where personal data are collected from the data subject”
Article 14: “Information to be provided where personal data have not been obtained from the data subject”

Scenario: “*A department manages a team of subject matter experts and contractors who are available for a number of projects and operations at UCL. The department keeps the following data on a spreadsheet stored on the N: Drive, and a copy on UCL SharePoint and on a 3rd party Resource Pool portal:*

The department receives this information from the department’s resource management team who manages the recruitment process. In addition, the department has a resource pool shared mailbox.”

Data collected	GDPR Data Type
Name	Personal information
Job title	Personal information
Finance code they are charged to	Non-personal information
Their taxation and IR35 status	Personal information
Their charge rates (salary)	Personal information (best treated as confidential)
Their contract end date	Personal information
Their employment status.	Personal information
Photo (optionally provided)	Personal information
Disability information	Special category personal data
Equalities	Special category personal data

This scenario presents several GDPR concerns, however, prior to assessing these, there are some general queries which need to be addressed first:

Query 1: When the data was collected by the resource management team, was this collected according to the Data Protection Act (DPA) 1998?

Query 2: Are you using any of the collected information for any other purposes (e.g. secondary processing such as newsletters to these individuals, marketing or other business analysis)?

Query 3: How long are you retaining the data for?

As part of GDPR you need to be open with individuals when you collect their data about how it will be gathered and used. They must be informed about what you are collecting, why you are collecting it, how you will process it, how you are retaining it, and how long you will retain it for.

STORAGE QUERIES:

Query 4: You note that this is stored on a managed portal, as well as on a spreadsheet and the N: Drive - What is the reason for this duplication?

Query 5: Who has access to this spreadsheet?

GDPR prescribes that you should not duplicate data unnecessarily. In this example, the triplication of the data in a portal, SharePoint and on the N:Drive has increased the risk of breach by creating multiple copies of the same file.

GDPR gives individuals rights to access their data. If data is duplicated in other areas it becomes increasingly harder to identify where their data is stored in the event of a Subject Access Request (SAR).

Query 6: Do you consider the information and the processing that is being done to be 'high risk'?

Query 7: Have you completed a Data Privacy Impact Assessment (DPIA) and/or an Information Risk Review?

In this case study, we asked questions which are standard and generic in many situations. There are three primary concerns in this scenario:

1) **The manner in which the data was collected when originally gathered**

2) **The duplication of personal data**

3) **The access levels to this data**

Solution: If no DPIA (or similar risk review) has been completed, one should be completed as soon as possible. This will allow the department to understand the level of risk to privacy. Once identified, the processes and design can be adjusted to meet the privacy requirements.

When completing the DPIA, your interpretations and decisions should be documented, and you should revisit the DPIA at regular intervals to ensure continued compliance, including alignment with UCL's Records Retention Schedule and what was communicated to the individuals at the time of collection.

www.ucl.ac.uk/library/docs/retention-schedule.pdf

In circumstances where you are duplicating personal data, you should review the reasons for this duplication – there are scenarios where this is inevitable, however, you should aim to reduce duplication wherever possible.

7. CASE STUDY 2: MANAGING A CONTACT MAILING LIST

Linked to the 'integrity and confidentiality' principle in GDPR and how compliance with Articles 24 and 32 is achieved.

Article 24: "Responsibility of the controller"

Article 32: "Security of processing"

Scenario: "I manage a number of events whereby members of the public, as well as UCL staff, are invited. I have a contacts mail list which I inherited from my predecessor, with the following fields.

I ask attendees to fill in a sheet at the door with their contact information so that I can send them a newsletter; this newsletter is sent using MailChimp. I am using Google Drive to store these contact lists and other details, and this is shared with my team."

Data collected	GDPR Data Type
Name	Personal information
Surname	Personal information
Job title	Personal information
Email	Personal information

This scenario presents several GDPR concerns. Prior to assessing these concerns,the individual must transfer all this data to UCL Managed Services, and securely delete this information from the Google Drive.

UCL cannot secure, catalogue, and retrieve UCL data if it is not on UCL Managed Services

In parallel to the securing of the data the following queries need to be addressed:

Query 1: When the data was originally collected was this collected according to the Data Protection Act (DPA) 1998?

Query 2: Are you using any of the collected information for any other purposes? (e.g. secondary processing such as newsletters to these individuals, marketing or other business analysis)?

Query 3: Are you retaining the data in line with UCL's Records Retention Schedule

www.ucl.ac.uk/library/docs/retention-schedule.pdf

If the answer to any of the three queries is 'no / yes / no', a Data Protection Impact Assessment (DPIA) should be completed to assess the level of risk to privacy. The DPIA will identify the level of risk to individual's privacy. Your response to the risk identified in the DPIA must be proportionate to the level of risk.

MailChimp is a common 3rd party mailing system that is in widespread use. Usually, staff upload a master spreadsheet of contact details to MailChimp to send out bulk e-mails. However, there are two issues which users need to be aware of with this practice:

1) MailChimp's servers are in the United States (US) and therefore by using this service you are transmitting personal data outside of the EU/EEA – If you have not informed individuals whose data you hold that this is taking place, you have not met your GDPR requirements.
2) When an individual 'unsubscribes' the MailChimp database is updated – if you do not undertake a regular reconciliation procedure, your master spreadsheet will not be accurate and therefore you have not met your GDPR requirements.

FUTURE COMPLIANCE WITH GDPR:

- When inviting individuals to events, you need to ensure that you provide a Privacy Notice outlining what data you are collecting, for what purpose and how long you will retain it.
- You need to ensure that you have put processes in place to ensure that data is collected appropriately, and that should an individual revoke their consent and ask for the data to be removed then this is able to be undertaken.

Focusing on the processing of personal data collection upfront and presenting correct privacy notices and storage of data under GDPR will reduce the risk of downstream activities and processing

APPENDIX A – KEY TERMS

TERM	DEFINITION
Anonymisation	The process of turning data into a form which does not identify individuals and where identification is not likely to take place. This allows for a much wider use of the information. The Data Protection Act controls how organisations use 'personal data' – that is, information which allows individuals to be identified.
Consent	Consent must be freely given, specific, informed and an unambiguous indication of the individual's wishes. There must be some form of clear affirmative action (positive opt-in), consent cannot be inferred from silence, pre-ticked boxes or inactivity. If an individual wishes to withdrawn their consent, the way for them to do so must be simple.
Controller	Decides how and why personal data is processed, determines the purposes and means of the processing of personal data.
DPA 2018	UK Data Protection Act 2018.
DPA 1998	UK Data Protection Act 1998.
DPIA	DPIAs (also known as privacy impact assessments or PIAs) is an assessment that is undertaken to identify potential areas of non-compliance and minimise risk.
DPO	Data Protection Officer.
GDPR	EU General Data Protection Regulation 2016.
Individual Rights	GDPR introduces 8 individual rights: 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, and Rights in relation to automated decision making and profiling.
Personal Data	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.

Principles of GDPR	Lawful, fair & transparent;
	Purpose limitation;
	Data minimisation;
	Accuracy;
	Storage limitation;
	Integrity & confidentiality, and
	Accountability

Processor	Acts on the Data Controller's behalf. This is often a third party.
Pseudonymisation	The processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.
Special Categories Personal Data	Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

CONTENTS ◀ ▶

APPENDIX B – USEFUL RESOURCES

DPA 2018	http://www.legislation.gov.uk/ukpga/2018/12/contents/enacted/data.htm
GDPR Regulation	https://www.eugdpr.org/
ICO	
Privacy notices	https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-notices-transparency-and-control/privacy-notices-under-the-eu-general-data-protection-regulation/
Lawfulness	https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/
12 Things to Do Now	https://ico.org.uk/media/1624219/preparing-for-the-gdpr-12-steps.pdf
GDPR Articles and Recitals	http://www.privacy-regulation.eu/en/
Health Research Authority	
Operational guidance -	https://www.hra.nhs.uk/about-us/news-updates/gdpr-guidance-researchers/
JISC	https://www.jisc.ac.uk/gdpr
Records retention schedule	Records retention schedule - http://repository.jisc.ac.uk/6254/1/hei-rrs.xls
UCL	
UCL Data Protection	https://www.ucl.ac.uk/legal-services/data-protection-overview
UCL GDPR website	www.ucl.ac.uk/gdpr
UCL GDPR DPIA	https://www.ucl.ac.uk/legal-services/ucl-general-data-protection-regulation-gdpr/guidance-notices-ucl-staff/data-privacy-impact
UCL GDPR Guidance Notices	https://www.ucl.ac.uk/legal-services/ucl-general-data-protection-regulation-gdpr/guidance-notices-ucl-staff
Records retention schedule	https://www.ucl.ac.uk/library/docs/retention-schedule.pdf
UKAN (UK Anonymisation Network)	http://ukanon.net/about-us/ukan-activities/
Article 29 Working Party Opinions	http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm
Anonymisation	http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf
Legitimate interests	http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf
Controller and Processor	http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf
For guidance on consent, portability, automated decision-making, privacy impact assessment	http://ec.europa.eu/newsroom/article29/news.cfm?item_type=1360

UNIVERSITY
COLLEGE
LONDON

CONTACT:

EMAIL: GDPR@ucl.ac.uk
WEB: www.ucl.ac.uk/gdpr

Design by UCL Health Creatives 2018