Imperial College Union

GDPR Assessment and Roadmap

Version Control			
Version	**Author**	**Date**	**Changes**
V1	Ashley Cory	14/05/2020	N/A

Imperial College Union EPOS Supply Options Appraisal

Contents

1. Overview

This document is designed to provide a general assessment of General Data Protection Regulations (GDPR) compliance and risk for Imperial College Union (ICU).

It will define what is required of an organisation to be GDPR compliant and highlight where ICU has areas of strength or where improvement is needed. It will then set out a proposed roadmap of improvements required to avoid risk of non-compliance. Although separate, this document will also reference the Privacy and Electronic Communications Regulations (PECR).

2. Requirements for Compliance

For the purposes of this assessment, ICU will be considered a 'Data Controller' and the list of general compliance areas below reflect that role.

Compliance areas are defined in the subheadings below with a short breakdown of required actions and are largely derived from standard guidance issued by the Information Commissioner's Office (ICO). Further reading has been referenced in the appendix of this document.

2.1 Lawful Basis for Processing

2.1.1 Information Asset Register

We must have documented where any personal or special category data is stored and how it is processed in an Information Asset Register (IAR). An IAR should define:

- Lawful basis of which we store/process data records
- Who has access to data records
- Retention periods and deletion schedules of data records

2.1.2 Privacy Notice

We must also have detailed the purposes and the lawful basis of our data storage/processing in a privacy notice that should be communicated to data subjects. Different data subjects may require different privacy notices.

2.2 Individual Rights

2.2.1 Exercising rights

We must make it clear to any data subjects that they can exercise their rights under GDPR (see appendix document 'General guidance for Data Controllers from ICO' for more details on these rights).

2.2.2 What we hold

We must provide information clearly detailing all the information under the above 'Lawful basis for processing' and communicate it to data subjects. This is usually in included in a privacy notice or policy.

2.2.3 *Processing requests*

We must have a clear process to allow data subjects to make requests under their Individual Rights and we must have a clear process for completing such requests within one month.

2.3 Accountability and Governance

2.3.1 *Accountability*

We must have an appointed Data Protection Officer and someone within the organisation designated as responsible for GDPR compliance.

2.3.2 *Governance*

We must have a clear data protection policy. This policy should clearly document our operational processes and technical measures in place surrounding GDPR compliance and who is responsible for these processes. Any policy must be regularly reviewed and audited to ensure it is still relevant and fit for purpose.

2.3.3 *Data breaches*

We must have a clear process documented and in place surrounding recording, mitigating against and reporting data breaches.

2.3.4 *Data Protection Impact Assessments*

We must have a clear policy on when we conduct a Data Protection Impact Assessment (DPIA) and detailed a clear internal process of how we conduct a DPIA.

2.3.5 *Training*

General GDPR training should be in place for anyone that has access to our data and training completion should be regularly audited and tracked. Training content should be regularly reviewed.

2.3.6 *Data Sharing Agreements*

We should have Data Sharing Agreements in place with any third parties that we share personal or special category data with (including Imperial College London).

2.4 Security

2.4.1 *Security processes*

We must have a demonstrable process in place to ensure the security of our stored/processed data including that passed to third parties. This can include penetration testing where appropriate or the pseudonymisation or anonymisation of data.

2.4.2 *Security policy*

Our processes ensuring data security should be clearly documented as part of general GDPR policy.

2.5 Other Considerations

2.5.1 Privacy and electronic communications regulations (PECR)

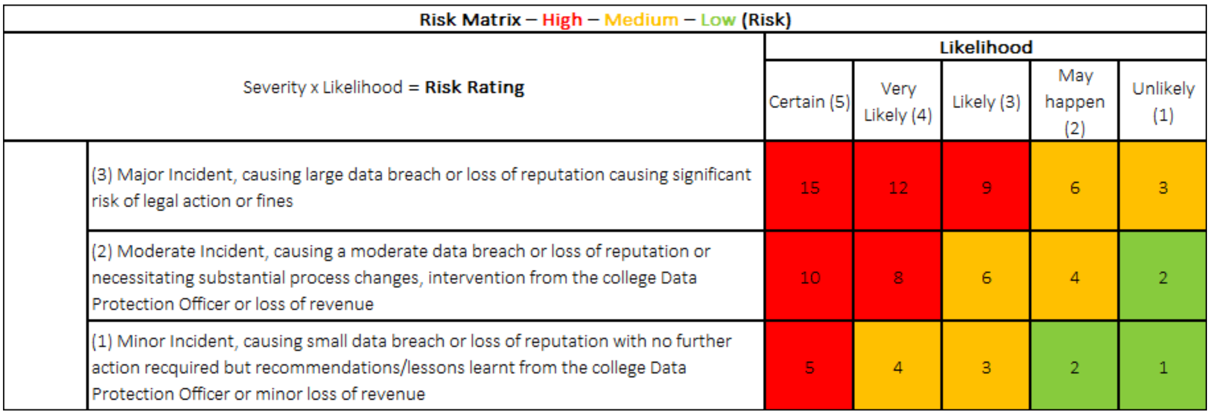
While not technically part of GDPR it should be considered as part of general measures put in place to ensure GDPR compliance. We must ensure that when conducting marketing communications we obtain the appropriate level of consent when generating mailing lists.

2.5.2 Good practice advice

We should have good practice advice/resources for all staff that process/store data. An example could include email inbox guidance, or safety tips surrounding ICT usage.

3. Risk Assessment

Please note, that in this document, where risks are determined, they are calculated by taking the scenario of being audited by an external source reporting to the ICO or by considering risk of data breach. Assessment uses the following risk assessment matrix:



Risk Matrix – **High** – **Medium** – **Low** **(Risk)**						
Severity x Likelihood = **Risk Rating**		**Likelihood**				
		Certain (5)	Very Likely (4)	Likely (3)	May happen (2)	Unlikely (1)
	(3) Major Incident, causing large data breach or loss of reputation causing significant risk of legal action or fines	15	12	9	6	3
	(2) Moderate Incident, causing a moderate data breach or loss of reputation or necessitating substantial process changes, intervention from the college Data Protection Officer or loss of revenue	10	8	6	4	2
	(1) Minor Incident, causing small data breach or loss of reputation with no further action recquired but recommendations/lessons learnt from the college Data Protection Officer or minor loss of revenue	5	4	3	2	1

4. Current State of Operation

4.1 Overview

What we currently have documented and in place.

4.2 Lawful Basis for Processing

4.2.1 Information Asset Register

Currently, ICL maintain an all-college Information Asset Register that makes use of a system that records data records**.** There is some question as to whether this system is fit for purpose and is currently under review.

ICU has mostly documented the personal and special category data that it holds. However, there is some confusion surrounding our use of the ICL IAR. ICU does have a very small number of records (less than 10) present in the ICL IAR, but these are certainly incomplete and not representative of our practices.

We also have a far more comprehensive IAR stored separately to the college, which they do not have visibility of and is named ‘ICU Data Audit’. It is basic in format (Excel). This document was last edited in 2019 and needs review but is generally representative of our practices.

Our IAR records generally records the necessary information expected of an IAR but is not clear on who within ICU can access specific records. Data retention schedules are recorded but may not be enforced. Our retention schedules for some records have been questioned by the college Data Protection Officer in the past.

Risk and proposed improvements

The above issues identified are classified as **medium** risk (6).

Improvements:

- Agree with the Data Protection Officer where our IAR records should be held (use of ICU IAR is recommended but with visibility given to Data Protection Officer)
- Ensure all records are in one place
- Review IAR and update to improve information on access rights
- Review and agree retention schedules with the Data Protection Officer
- Implement process to enforce retention schedules

4.2.2 Privacy Notice

ICU currently has three privacy statements, displayed via eActivities and the dotorg website:

General

The general privacy statement covers data held for students, staff and members of ICU. It is extensive and generally robust. It covers legal rights of data subjects and details the lawful basis on which we hold data. We do not have a defined schedule for review of this document.

The privacy statement is to be presented to students on first login to the dotorg website for acknowledgement.

Marketing

There is a short privacy statement for our Mailchimp newsletter recipients. This privacy statement is robust, although it states that we gain explicit consent via an opt-in mechanism. At present, we do not have an apparent opt-in mechanism for our Mailchimp newsletter, and only provide an opt-out mechanism.

Our newsletter mostly contains useful information for students regarding our services but may also include direct marketing such as event ticket sales, or reference to our retail and hospitality outlets.

Having no true opt-in process for newsletters that contain direct marketing is not legal under PECR and is advised against under college policy: https://www.imperial.ac.uk/communications/internal-communications/email-newsletters/legal-guidance/

Liberation Groups
There is a is a short privacy statement for our Liberation Groups newsletter recipients. This privacy statement is robust, and recipients join the mailing list via an opt-in mechanism found here: https://www.imperialcollegeunion.org/your-union/your-representatives/liberation-community-zones

This privacy statement is generally fit for purpose.

Risk and proposed improvements

The above issues identified are classified as **high** risk (9).

Improvements:

- Review and update all privacy statements
- Implement review periods for all privacy statements
- Review opt-in mechanisms for newsletter with college Data Protection Officer
    - Either split marketing into separate newsletter or review opt-in/out statement that recipients accept with the college to refer to our newsletter

4.3 Individual Rights

4.3.3 Exercising rights

As described above, our privacy statement makes clear reference to data subjects individual rights and that they can exercise them.

Risk and proposed improvements

The above issues identified are classified as **low** risk (1).

No further recommendations.

4.3.4 What we hold

We provide clear information detailing our lawful basis for processing the data of data subjects as part of our general privacy statement.

Risk and proposed improvements

The above issues identified are classified as **low** risk (1).

No further recommendations.

4.3.5 Processing requests

We have some inconsistency in providing a clear process for data subjects to exercise their rights. Our general privacy statement informs data subjects that:

‘If you want to review, verify, correct or request erasure of your personal information, object to the processing of your personal data, or request that we transfer a copy of your personal information to another party, please contact the College’s Data Protection Officer in writing.’

This is fine in principle, but we should also refer to the rights of access under the Subject Access Request process in the privacy statement, although we do already reference this on the privacy section of the dotorg website. We should also provide the method to contact the College’s Data Protection Officer. This can be found via the Imperial College website, but we do not link to it.

Both the privacy statement and the Imperial College website refer to a previous Systems Team Manager to contact for further information. Our privacy statement should be specific to role only to avoid outdated information.

Risk and proposed improvements

The above issues identified are classified as **low** risk (2).

Improvements:

- Implement general data protection policy (include responsibility, method of maintaining and processes of monitoring compliance)
- Review and update all privacy statements
- Implement review periods for all privacy statements

4.4 Accountability and Governance

4.4.1 Accountability

Our appointed data protection officer as is the same Officer as the college. However, we do not have a full data protection policy and we do not officially designate a staff member within ICU as being responsible for GDPR compliance.

There has been confusion over what staff members should be responsible for signing agreements with the college on data protection.

Risk and proposed improvements

The above issues identified are classified as **low** risk (2).

Improvements:

- Implement general data protection policy (include responsibility, method of maintaining and processes of monitoring compliance)
- Assign a member of assign a member of ICU Staff as a Data Protection Coordinator to officially liaise with Data Protection Officer (Systems Manager or appropriate member of ICU Leadership recommended)

4.4.2 Governance

While we have a robust privacy statement, we do not currently have a clear data protection policy.

Our privacy statement does in some cases go as far as stating that processes exist (such as for data breaches etc) but does not detail these processes or state responsibility for maintaining them.

We do not have clear processes in place to maintain our IAR or enforce retention schedules. Where policies do exist and are not centralised in a data protection policy (such as the data breach policy) we do not clearly communicate our policy to data subjects.

Risk and proposed improvements

The above issues identified are classified as **medium** risk (6).

Improvements:

- Implement general data protection policy (include responsibility, method of maintaining and processes of monitoring compliance)
- Review and agree retention schedules with the Data Protection Officer
- Implement process to enforce retention schedules
- Ensure all policy (internal and external) is collected and kept in a single central location
- Ensure all policy is clearly accessible to data subjects where appropriate
- Where internal policies exist, ensure that they are accessible to all necessary staff
- Ensure all policies have a regular review date

4.4.3 Data breaches

We do have a clear data breach policy that is robust and in line with the college data breach policy.

There are some elements of the policy that could be improved. Groups and forms used to communicate breaches have no process implemented to keep them updated.

We store our process documentation on data breaches in the Data Protection SharePoint. Access to this documentation is limited and not available to all internal staff. We do not make our process clear externally.

Risk and proposed improvements

The above issues identified are classified as **low** risk (2).

Improvements:

- Ensure that policy is accessible to all necessary staff
- Ensure policy is clearly accessible to data subjects
- Ensure policy has a regular review date
- Ensure process is put in place to keep groups and forms up to date

4.4.4 Data Protection Impact Assessments

We must have a clear policy on when we conduct a Data Protection Impact Assessment (DPIA) and detailed a clear internal process of how we conduct a DPIA.

We have no policy on when we conduct a Data Protection Impact Assessment (DPIA). We have no internal process relating to how we would conduct a DPIA. We have no process to enforce or audit the completion of DPIAs.

The college does have a clear policy and clear criteria for conducting a DPIA: http://www.imperial.ac.uk/admin-services/secretariat/information-governance/data-protection/processing-personal-data/data-assessments/

We do not refer to this policy in any documentation. We do have a copy of the college DPIA template in the Data Protection SharePoint folders, but this version is outdated and there is no process to ensure it is consistent with current college documentation.

We currently have not conducted a DPIA for any current or past projects.

Risk and proposed improvements

The above issues identified are classified as **high** risk (9).

Improvements:

- Implement general data protection policy (include responsibility, method of maintaining and processes of monitoring compliance)
- Implement internal process for enforcing and conducting DPIAs
- Conduct DPIAs for all recent and current projects that require one
- Ensure DPIA is regularly reviewed and kept consistent with college process

4.4.5 Training

We have two sets of training material. One located in the Data Protection SharePoint folders and is designed for face-to-face training. The other is in the e-Activities training hub and is designed for online self-service.

Both sets of training are robust in their content and cover all necessary basics for GDPR compliance.

The face-to-face training offers a quiz to assess trainee understanding of the content. The e-Activities training offers no interaction with the trainee and does not assess trainee understanding. Neither set of training enforces a pass rate.

Intended audiences for the training are unclear. Technically, both sets of training are or could be accessible to both ICU staff and to students operating in CSPs. Implicitly, both sets of training are aimed at just students operating in CSPs. We have little focus on training for ICU staff.

We have no discernible process in place to ensure that all ICU staff and students operating in CSPs take either the online training or have the face-to-face training delivered. We have no record of training completion and we have no method to audit completion rates among ICU staff or students operating in CSPs.

Risk and proposed improvements

The above issues identified are classified as **medium** risk (6).

Improvements:

- Implement general data protection policy (include responsibility, method of maintaining and processes of monitoring compliance)
- Review and update training material/content where necessary
- Implement review schedule for all training
- Ensure audience for training material is clear and that clear sets of training exist for officers, staff and students operating within CSPs with clear routes of access to training
- Implement and record pass rates and ensure process exists to conduct annual audit of at least officer and staff completion of training
- Incorporate face-to-face training into officer training and staff induction

4.4.6 Data Sharing Agreements

We do not currently have any data sharing agreements in place with external bodies or the college and/or have no place to centrally store or manage those data sharing agreements.

There is little transparency on where ICU might exchange data with other third parties. There may be further examples where ICU staff or CSPs exchange data with third parties as part of everyday operations with no agreements in place.

Risk and proposed improvements

The above issues identified are classified as **high** risk (9).

Improvements:

- Ensure completed DSAs are kept in a single central location and subject to a regular review schedule
- Create DSA template for general use by CSPs and/or ICU staff
- Audit CSP/ICU staff use of data and record all occurrences where data is shared
- Implement DSA with the college
- Implement DSAs with any other known third parties

4.5 Security

4.5.1 Security processes

We generally make use of college-managed infrastructure to hold much of our data and as such are generally secure. The Systems Team ensures systems are kept up-to-date and secure.

Currently, no anonymisation or pseudonymisation are implemented and we have no external penetration testing in place on our systems.

Risk and proposed improvements

The above issues identified are classified as **medium** risk (6).

Improvements:

- Implement general data protection policy (include responsibility, method of maintaining and processes of monitoring compliance)
- Liaise with college Data Protection Officer and college ICT to discuss resources and best practices surrounding data security
- Amend and update processes and policy where appropriate

4.5.2 Security policy

We have no general policy relating to GDPR and so do not detail our security processes.

Risk and proposed improvements

The above issues identified are classified as **medium** risk (6).

Improvements:

- Implement general data protection policy (include responsibility, method of maintaining and processes of monitoring compliance)

4.6 Other Considerations

4.6.1 Privacy and electronic communications regulations (PECR)

We currently do not ensure appropriate levels of consent when approaching mailing list recipients with direct marketing

Risk and proposed improvements

The above issues identified are classified as **high** risk (9).

Improvements:

- Review and update all marketing privacy statement
- Review opt-in mechanisms for newsletter with college Data Protection Officer
    - Either split marketing into separate newsletter or review opt-in/out statement that recipients accept with the college to refer to our newsletter

4.6.2 Good practice advice

We have some good practice advice in our training material, but this could be improved.

Risk and proposed improvements

The above issues identified are classified as **low** risk (2).

Improvements:

- Create good practice advice where beneficial and communicate it to ICU staff in an accessible manner

5. Recommended road map of proposed improvements

Some progress has already been made toward the above suggested improvements. For example, a Data Sharing Agreement is currently in final draft and currently under review by the college before signing. The Data Protection Officer has been engaged with the process of review and is open to helping and giving advice.

Much of the above improvements coalesce around the creation of a general ICU data protection policy. This can be achieved by either creating a policy exclusive to ICU, or by incorporating the college general policy found here: https://www.imperial.ac.uk/admin-services/secretariat/information-governance/data-protection/our-policy/

There are examples of Unions across the UK taking both approaches. An exclusive ICU policy is likely a more robust option, whilst adapting to the college policy is likely to require less resource.

Incorporating the college policy may necessitate changes to the policy and would be achievable only under agreement with the Data Protection Officer. Over the course of the interim plan leading up to the 2020/21 financial year, we should engage with the Data Protection Officer and agree the preferred approach.

It is recommended that the above suggested improvements be incorporated as part of the general 2020/21 plan following on from the interim plan projects leading up to the 2020/21 financial year.

Any quick win improvements that can be made immediately and with little resource could be implemented immediately during the period covered by the current interim plan.

2020/21 aims:

- Any identified high risks (privacy statements and marketing, DPIA process and Data Sharing Agreements) should be resolved in the first half of the 2020/21 financial year
- Any identified medium risks (IAR, policy review, training framework and security processes) should be resolved by the end of the 2020/21 financial year
- Any identified low risks should be considered nice to have and implemented if resources allow

The ultimate outcome of the 2020/21 financial year in relation to data protection should be the creation of a general ICU data protection policy with a regular review period, detailing clear internal and external processes and how we enforce/monitor those processes. If we decide to make use of the college general policy, then internal processes need to be made and enforced to match that policy.

Appendix

General guidance for Data Controllers from ICO: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/

General guidance for Data Controllers from the EU: https://gdpr.eu/checklist/

College legal guidance on newsletters: https://www.imperial.ac.uk/communications/internal-communications/email-newsletters/legal-guidance/

Opt-in for liberation groups: https://www.imperialcollegeunion.org/your-union/your-representatives/liberation-community-zones

College DPIA: http://www.imperial.ac.uk/admin-services/secretariat/information-governance/data-protection/processing-personal-data/data-assessments/

College general data protection policy: https://www.imperial.ac.uk/admin-services/secretariat/information-governance/data-protection/our-policy/