General Data Protection Regulations (GDPR)
Guidance on storing HR data

Contents

---

1. Introduction

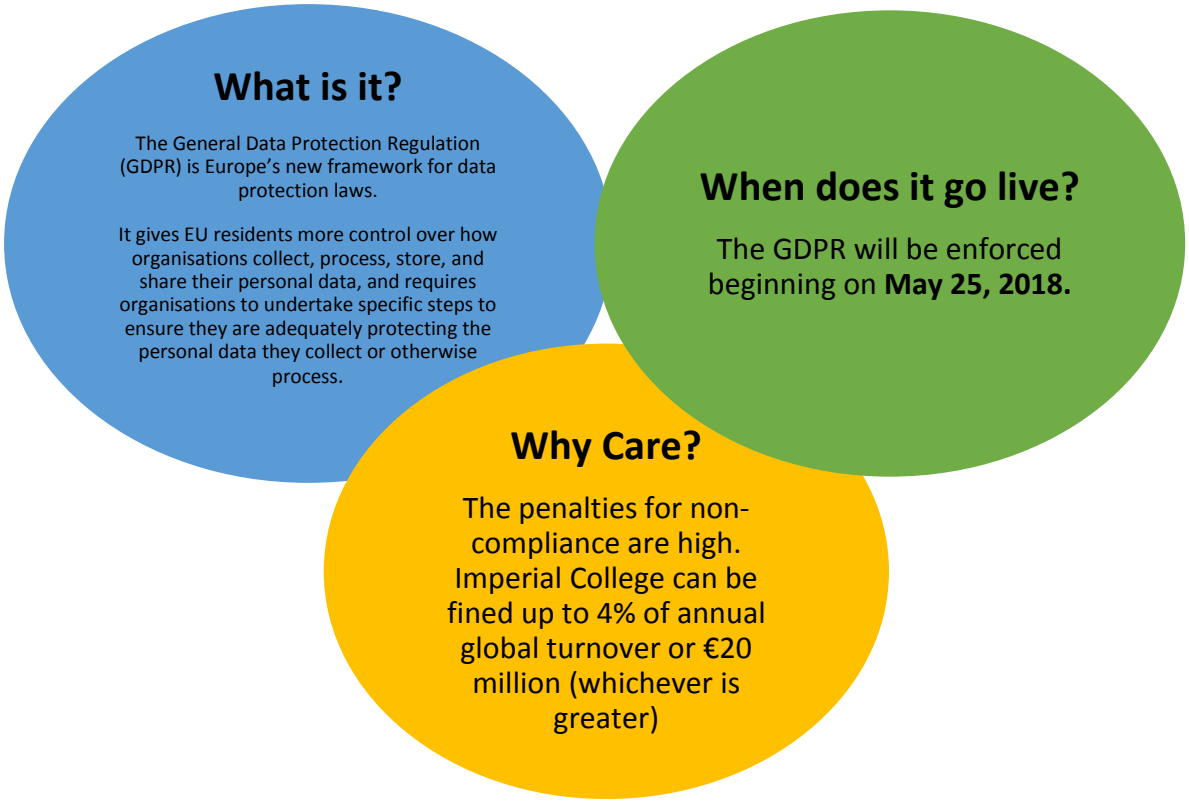
This guidance is designed to assist you with meeting GDPR guidelines when handling HR data, for example, during the recruitment process, employment life cycle, employee relations processes or when using HR Management Information reports.

It is applicable to all staff who are either involved in the above mentioned processes and/or who have access to data/reports produced and issued by the HR Management Information team.

It should be read in conjunction with the GDPR information contained on the College's Legal Services' webpage and the College's Retention Schedule.

May 2018
Updated August 2018

2. GDPR Fundamentals



Who does it affect?

Data Controllers – Imperial College is the data controller. The GDPR requires compliance from any organisation that collects personal data from someone in the EU.

Data Subjects – refers to the individual who is providing their personal data to Imperial College.

Data Processors – this is applicable to anyone involved in an HR process since they are responsible for processing personal data on behalf of the Data Controller. They have a legal obligation to comply with the GDPR.

3. Recruitment

These guidelines are applicable when:

- Applications are received outside of the College's Applicant Tracking System (ATS), TalentLink - i.e. applicant data received via referrals, agencies or direct sourcing
- Shortlisting
- Interviewing
- Referencing

- On-boarding

To ensure GDPR compliance you should:

✓ Upload all applicant/candidate data (e.g. applications received for agencies, applicants emailed directly to you) to the College's ATS wherever possible. When doing so, **always** ensure that the data subject (applicant/candidate) has been notified that their data has been uploaded. Further information on how to manually upload candidates can be found at the **Recruitment & Selection Procedure web page.**

✓ Where possible, login to the College's ATS to view all applicant/candidate data (i.e. CV, cover letter, references, research papers etc.)

✓ If considering an applicant/candidate for an alternative requisition, **always** ensure consent has been obtained to do so. The College's ATS will alert you if the applicant/candidate hasn't provided consent to be part of our Talent Pool.

✓ If using portals such as LinkedIn, share speculative profiles with HMs within the portal; obtain full consent from potential applicants/candidates before forwarding their data outside of the portal

✓ Only approach referees if the applicant/candidate has provided consent on their application

✓ Only approach applicant/candidate referees when referencing information is required i.e. if a provisional offer has been made or if the candidate is being invited to interview

✓ If applicant/candidate data is downloaded, store it on College secure drives and archive when it is no longer required

✓ Delete all copies of applicant/candidate data from email chains once no longer required

✓ Only send applicant/candidate data to those recipients who are directly involved in the recruitment

✓ Include wording within your email signature and relevant templates to advise recipients to delete applicant/candidate data once processed (see below) or if data is sent in error

✓ Take the opportunity now to cleanse all files and email inboxes which may contain expired applicant/ candidate data

✓ Dispose of all hard copy applicant/candidate data in confidential waste when no longer relevant

Further information

Please also view the resources and guidance at section 7 below.

If you have any further questions on GDPR compliance during recruitment, please contact recruitment@imperial.ac.uk and include GDPR in the email subject line.

4. Employment life cycle data

To ensure GDPR compliance you should:

✓ For all HR correspondence, templates, forms etc. that may be transmitted by email during an individual's employment at the College, refer to the College's GDPR guidance webpage on emails: http://www.imperial.ac.uk/admin-services/legal-services-office/data-protection/internal-guidance/guide-1---e-mail/ . If storing such emails locally please do so in line with the College's Retention Schedule.

✓ Ensure staff records are stored in a secure place (locked cabinet, properly secured electronic environment that is approved and guaranteed by the College's ICT Department).

✓ Only retain essential information on staff files.

- ✓ After staff leave College employment, retain files for no longer than the period outlined in the College's Retention Schedule and request that ACRU dispose of staff files at the relevant time.
- ✓ Please note that: staff records of Senior Staff may be retained indefinitely for historic purposes.
- ✓ Dispose of all hard copy data in confidential waste when no longer relevant
- ✓ Limit access to staff files in accordance with current HR policies and procedures.
- ✓ Inform staff that they have a right to access their personal information and explain how their data will be used, processed and stored.
- ✓ Include wording within your email signature and relevant templates to advise recipients to delete data once processed (see section 6 below) or if data is sent in error.
- ✓ May share information about staff with their home departments if specifically requested for departmental business processes and record-keeping purposes. This information must be protected by Windows Rights Management or password (please see section 5 for more information on protecting documents).
- ✓ Do not share or send spreadsheets internally or externally containing staff information unless data is anonymised (except as noted above).

Further information

The College's Data Protection guidance webpages provide further information and in particular you may wish to refer to:

- **Guide 7 – Preparation and Disclosure of References**
- **Guide 9 – Disclosure of staff personal data to third parties**

Please also view the resources and guidance at section 7 below.
If you have any further questions in relation to processing staff data, please contact your local HR representative and include GDPR in the email subject line.

5. Employee Relations data

Disciplinary information

The College retains disciplinary documentation which records any warnings issued and or capability issues including a summary of future behavioural expectations.

Disciplinary and Grievance Investigation paperwork

The College retains a record of any investigations that have been carried out in relation to the person being investigated.

The following is potentially the type of information that HR will retain in relation to ER issues:

Disciplinary Issues

- Details of the allegations
- Supporting witness statements
- Investigation report
- Invite to disciplinary hearing
- Occupational Health reports and other medical evidence

- Comparative data with other members of staff
- Notes of disciplinary hearings
- Details of other disciplinary issues
- Details of other disciplinary hearings
- Copies of other warnings
- Outcome of disciplinary hearings
- Letter of Appeal
- Appeal Investigation paperwork
- Notes of appeal hearing
- Outcome of appeal

Grievance Issues

- Details of grievance
- Supporting witness statements
- Investigation reports
- Notes of meetings with individual and any witnesses
- Outcome of grievance hearing
- Appeal of grievance
- Notes of appeal
- Notes of meetings with witnesses to appeal
- Outcome of appeal

Similar documentation will be retained for Scientific Misconduct Investigations.

To ensure GDPR compliance you should:

- ✓ As a member of the disciplinary panel, only retain the information provided in relation to the disciplinary until issue of the outcome of the Hearing*
- ✓ As the Investigation Officer, only retain paperwork relating to an investigation until the investigation report has been issued*

***information will be stored centrally as mentioned higher up in this section.

6. HR Management Information (HRMI)

The HR Management Information team produce the following report types:

Report type	Description	Protection	How report is issued
Regular	Specific report types produced on a pre-set basis and issued to a specific group of individuals	All reports are normally either Window Rights Management or password protected. Non sensitive and anonymised information is not normally protected.	SharePoint and/or email
Ad-hoc, external and Freedom of Information requests	Produced as required and are assessed on a case-by-case basis.		Email or by secure portal

Protection of HR Management Information data:

<u>Windows Rights Management (WRM)</u>

WRM is a tool that provides encryption and control of document distribution to users of Microsoft Office. The document is accessible only by those named in the email distribution list.

Each report and its accompanying text are confidential and its contents are intended only for the individual(s) to whom it is addresses. Unauthorised disclosure, copying or distribution is strictly prohibited. Our full data protection policy is available to view.

WRM allows us to restrict access to the report to a list of designated named users/email addresses provided by the report creator. Permission is restricted and report recipients are given Change access. Users with Change permission can read, edit, copy content from, and save changes to the workbook. They are also given access to print content. If the report is forwarded on to somebody who is not on the list of users who have been given permission, or someone outside of the College network, that person will not be able to open the file. In either of these cases, an error message will appear advising the person to contact the report creator.

Reports emailed out using WRM will clarify this on the email and those uploaded to the HR Management Information site will always be protected with WRM.

Passwords

In the case that the report recipient cannot access WRM-protected files (e.g. Mac users, external recipients, etc), the HRMI team protect the file using a password. For regular reports, this password is in a pre-decided evolving format that is known to the recipients. For ad hoc reports, the password is set by the report creator on a case-by-case basis.

To ensure GDPR compliance you should:

- ✓ Appropriately protect any report you receive when saving or sharing it locally
- ✓ Never forward a password to another individual in the same email the report is attached to
- ✓ Contact hrreportrequest@imperial.ac.uk if you need to disseminate the contents of a report protected by WRM further to approved team members, or if you are a new member of staff who needs access to the reports going forward
- ✓ Refer to the WRM webpage for further information on this topic
- ✓ Read the guidance on the ICT webpages on protecting sensitive data and the Be Secure page for IT security information

If you have any queries on the information provided in section 6 of this document, please contact: hrreportrequest@imperial.ac.uk

7. Resources and additional guidance:

The table below provides recommended wording to add to emails, this text should be edited as suggested and as relevant for the email contents.

Forwarding data - recommended wording	*This email contains personal data. We request that it is treated confidentially at all times and is not distributed to a wider group of*

	individuals than necessary. To comply with the GDPR, please delete this email when the data is no longer relevant.
Email signature confidentiality - recommended wording	*Any information contained herein is intended only for the named recipient and is to remain confidential and under no circumstances should it be distributed, disclosed, copied or transmitted to other parties without the express permission of Imperial College London. If you are not the intended recipient please notify the sender immediately and delete this email from your system.*
Immigration and Disclosure and Barring Service record keeping requirements	Please visit the **Recruitment and Selection Policy** and see the above guidelines regarding storing data on secure drives