THE LONDON SCHOOL OF ECONOMICS AND POLITICAL SCIENCE

Operational

How to apply the Data Protection Principles in your work

Guidance for Staff

There are six data protection principles in the General Data Protection Regulation (GDPR) that determine how we should be treating personal data. They can appear theoretical at first sight. This guidance goes through how you can apply the principles in your work.

Principle 1 - processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency')

Question to consider: Would I want my personal data treated this way?

Main points of this principle: lawfulness, fairness and transparency.

Lawfulness means that you are processing the data under one of the lawful bases allowed in the GDPR. So when we process most student data, this is due to the contract lawful basis because the student signs a contract with the School (conditions of registration) in order to obtain the service of education. We keep next of kin details under vital interests because in a life or death situation we need to be able to let a student or staff member's family know of the problem. We have a legitimate interest in contacting alumni, so can use that lawful basis for holding that data.

Fairness means treating the data as you would like your own to be treated. It means taking care that you are sending data to the right person, that you only share it with those who need to know, that you consider if what you are doing with the data is something the individual it is about would like to happen.

Transparency means being upfront with what you are doing with personal data. This means giving research subjects information on how their data will be used in your research. It means giving people the information they need to withdraw consent for processing or to ask for their information. It means letting people know if you are automatically processing their data. It means keeping your information asset register up to date so we can tell people what we do with the data we hold on them. It means that we have a set of general privacy notices available on the website so different groups know what data we process relating to them e.g. students, staff.

Principle 1 take aways:

Identify a lawful basis when you are processing personal data.

- Consider how you would want your data processed if you were the data subject.

- Be transparent with data subjects about how you will process their data.

Principle 2 - 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, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');

Question to consider: Why does this process need personal data?

Main points of this principle: Identifying why you need to collect personal data – specifically, explicitly, with a legitimate purpose and not further processed for a completely different purpose. Does not apply to data being reused for research.

Specific and explicit purposes mean that you have identified a process that needs personal data in order to function. For example, to process a student application, you will need certain data about that individual to know whether they are a good fit for the course.

Legitimate purpose means that you have a reasonable need for the data. For example,

we cannot process a student application with a blank piece of paper, we have a legitimate requirement to collect certain data to make the assessment on their fitness for a course. We have a legitimate requirement to mark their work and collect those marks in order to determine if they have reached the level required to receive a degree.

Not further processed for a completely different purpose means we can't take student application data and then use that data to sign them up for every newsletter the School produces. We could however, re-use the data they have supplied if they decide to apply for another course.

However, data collected for one purpose can be reused for research. The 'not to be considered to be incompatible with the initial purpose' should cover most research. Possibly if research would interfere with the original purpose, it would be incompatible, but without further guidance in this area yet, we can consider it an exemption that could be used by most if not all research at the School.

Principle 2 take aways:

- The process determines if you need personal data, not the other way around
- You should be able to identify a legitimate reason why we need the personal data for the process
- Data collected for one purpose should not be used for another incompatible process
- UNLESS it is being used for research.

Principle 3 - adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation')

Question to consider: What do I need this data for?

Main points of this principle: data is adequate, relevant and only what is necessary for the task.

Adequate means that you have identified the minimum amount of data you need for a

particular task. For example, you won't be able to process exam marks without the candidate number. You won't be able to collect data on someone's opinions without actually collecting the opinion. If you need the personal data to do a particular task, this principle allows you to collect it.

However, it does need to be relevant for the task. If you do not need a data subject's grandmother's birth date for a task, do not ask for it.

When it comes to what is necessary, think about what you actually need for the task e.g. will student number do or do you need the candidate number as well. If you need the candidate number, use it. If you don't, use just the student number.

Principle 3 take aways:

- Do you need the personal data to do the task? If yes, collect and use it.
- If you do not need the personal data for the task, do not collect or use it.

Principle 4 - accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');

Question to consider: Do I have the correct data?

Main points of this principle: Keep data accurate and up to date where necessary. Be able to correct or delete inaccurate data.

Keeping data accurate means that it should correspond with reality. Sometimes this is easy – my name is Rachael Maguire, it says so on my passport and birth certificate. Sometimes this is not so easy – person A views an event occurring in one way and person B another. Which is the accurate version? You would be able to keep both as an accurate version of what both A and B thought they saw.

Up to date where necessary means that if data changes, you should update it e.g. I've got married and my new surname is Smith. However, sometimes you will take a snapshot of a point in time e.g. 'on 31st December 2017 my new year's resolutions

were...' which you would want to keep to compare the next December. If someone changed their mind in February, you would still want to keep the 31st December data. As such, it would not be necessary to change it. You may also take some interview notes which you then share for accuracy with the interviewee. They may say that they said something completely different to what you remember or recorded in the interview. You can keep their opinion on what they said with the original transcript but do not have to update the transcript.

You should be able to correct or delete data in line with the data subject rights in the General Data Protection Regulation. This could be a simple updating a misspelling e.g. it is Rachael not Rachel. Or it could be a more involved delete that opinion you recorded, which we may or may not do depending on what lawful basis it was collected under. For example, a witness statement that we need for legal purposes we would refuse to delete. But we should be able to tell people whether we will or won't delete within one month.

Principle 4 take aways:

- Accurate data corresponds with reality. If you have more than one view on reality, you can keep all.

- Data should be kept up to date where necessary, but does not always need to be corrected.

- You can keep a note of the data subject's difference of opinion with the original data.

- Inaccurate data should be corrected or deleted as necessary. However, we can refuse under certain circumstances.

Principle 5 - kept in a form which permits identification of data subjects for no longer than is necessary 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 in accordance with Article 89(1) subject to implementation of

the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation').

Question to consider: How long do I need to keep this data for?

Main points of this principle: If you can identify the individual, destroy the information as soon as you no longer need it. This does not apply to research data.

Kept no longer than necessary means that you destroy personal data in line with the School's retention schedules/the time limits shown in your information asset register entry. Destruction means complete deletion if electronic (so off backups as well) and shredded if paper (this includes the confidential waste sacks provided by the School).

However, this is principle also details whether it is kept in a form which permits identification of a data subject. Anonymised data can be kept longer. So if the original data has been deleted but has fed into anonymised statistics, you can still keep the statistics.

Like principle 2, there is an exemption for research data as long as you have safeguarded the rights and freedoms of the data subject. This means keeping the data secure (see Principle 6) while you are holding it and being able to provide access, correct and delete the data as requested by the data subject. Having done this, you can keep data for future research, even if you are not sure exactly what you will use it for in the future.

Principle 5 take aways:

- Destroy personal data you no longer need in line with the retention period for that data.
- If it is anonymised, you can keep it longer.
- You do not have to destroy data you may use in further research, but do have to keep it secure and respond to data subject requests relating to it.

Principle 6 - 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')

Question to consider: Could someone get to this data even if they should not?

Main points of this principle: Appropriate security includes protection from unauthorised or unlawful processing, accidental loss, destruction or damage. This can be done with appropriate technical and organisational methods.

So personal data should be kept secure, but what does this mean?

First, we have to avoid the following. Unauthorised or unlawful processing would cover processing of personal data that was not required by the School, but using data held by the School. So if someone hacked into the School's systems or used data inadvertently sent to them for their own purpose rather than deleting it. Accidental loss, destruction or damage would occur if for example a laptop got stolen or if data was destroyed or damaged before its retention period was reached.

So what are appropriate technical and organisational methods?

- Keep to the iron rules of information security (on this page: Cyber Security & Risk (lse.ac.uk))
- Encrypt data in transit
- Keep a clear desk policy – tidy all paper away at the end of the day in lockable cupboards
- Use SharePoint and OneDrive for cloud storage and external collaborator accounts for sharing
- Do the online information security course in Moodle Principle 6 take aways:
- Breaches to security include unauthorised or unlawful processing, accidental loss, destruction or damage
- Follow information security rules and procedures to ensure these breaches

do not occur.

Accountability principle

Question to consider: If someone asked me what I was doing with their data could I tell them?

Main points of this principle: To be accountable to data subjects and the Information Commissioner's Office about what we are doing with personal data.

This is not one of the six main principles, but underpins them all. It is the reason we have to keep records about personal data using the Information Asset Register. It is the reason we have to provide consent forms and other privacy notices. It is the reason that we provide information about making a request relating to personal data. It is the reason we will comply with the ICO when they request information regarding how we have handled a request or in processing data.

Accountability Principle take aways:

- Let people know what you are doing with their data
- Comply with requests from data subjects and the ICO
- Keep your IAR up to date.

Review schedule

Review interval	Next review due by	Next review start
3 years	30/06/2025	01/06/2025

Version history

Version	Date	Approved by	Notes
1	25/06/2018		
1.1	5/07/2022	IGMB	Minor changes

Links

Reference	Link

Contacts

Position	Name	Email	Notes
Information and Records Manager	Rachael Maguire	r.e.maguire@lse.ac.uk	

Communications and Training

Will this document be publicised through Internal Communications?	~~**Yes**~~**/ No**
Will training needs arise from this policy	~~**Yes**~~**/ No**
If Yes, please give details	