Data protection policy

Status: Draft

Version: 1.1

OID: 47934.6.1.2.3.01

2020-02-27

Contents

1 History

version	changes	approval date
1.0	initial policy	2019-01-28
1.1	rephrasing	draft

2 Scope

WPIA needs to gather and use certain information about individuals.

These MAY include customers, suppliers, business contacts, employees and other people the organisation has a relationship with or may need to contact.

This policy describes how this personal data MUST be collected, handled and stored to meet the organisation's data protection standards — and to comply with the law.

3 Why this policy exists

This data protection policy ensures WPIA:

- Complies with data protection law and follows good practice
- Protects the rights of staff, customers and partners
- Is open about how it stores and processes individuals' data
- Protects itself from the risks of a data breach

4 Data protection law

The General Data Protection Regulation (EU) 2016/679 ("GDPR")[^1] is a regulation in EU law on data protection and privacy for all individuals within the European Union (EU) and the European Economic Area (EEA). It also addresses the export of personal data outside the EU and EEA areas. The GDPR aims primarily to give control to citizens and residents over their personal data and to simplify the regulatory environment for international business by unifying the regulation within the EU. It describes how organisations — including WPIA — MUST collect, handle and store personal information.

These rules apply regardless of whether data is stored electronically, on paper or on other materials.

To comply with the law, personal information MUST be collected and used fairly, stored safely and not disclosed unlawfully.

Data protection follows the principle: “Data protection by design and by default”. This means, GDPR is underpinned by seven important principles. These say that personal data MUST:

1. Be processed fairly and lawfully
2. Be obtained only for specific, lawful purposes
3. Be adequate, relevant and not excessive
4. Be accurate and kept up to date
5. Not be held for any longer than necessary
6. Processed in accordance with the rights of data subjects
7. The responsible person is responsible for compliance with topics 1 to 6 and MUST be able to prove compliance on request (accountability).

5 People, risks and responsibilities

5.1 Policy scope

This policy applies to:

- The head office of WPIA
- All branches of WPIA
- All staff and volunteers of WPIA
- All contractors, suppliers and other people working on behalf of WPIA
- All fellows registered on the TERACARA portal

It applies to all data that the organisation holds relating to identifiable individuals, even if that information technically falls outside of the GDPR. This can include:

- Names of individuals
- Date of Birth
- Email addresses
- Level of education, expertise, skills, experience
- Payroll data
- Customer data, client data
- Postal addresses
- Email addresses

- Telephone numbers
- ... plus any other information relating to individuals

Not under this scope:

- Technology data
- Business data
- Strategic data

5.2 Data protection risks

This policy helps to protect WPIA from some very real data security risks, including:

- **Destruction**
- **Data loss**
- **Change of data**
- **Unauthorized disclosure, Breaches of confidentiality.** For instance, information being given out inappropriately.
- **Unauthorized access, Reputational damage.** For instance, the organisation could suffer if hackers successfully gained access to sensitive data.
- **Failing to offer choice.** For instance, all individuals SHOULD be free to choose how the organisation uses data relating to them.

5.3 Responsibilities

Everyone who works for or with WPIA has some responsibility for ensuring data is collected, stored and handled appropriately.

Each team that handles personal data MUST ensure that it is handled and processed in line with this policy and data protection principles.

However, these people have key areas of responsibility:

- The **board of directors** is ultimately responsible for ensuring that WPIA meets its legal obligations.
- The data protection officer is responsible for:
  - Keeping the board updated about data protection responsibilities, risks and issues.

  - Reviewing all data protection procedures and related policies, in line with an agreed schedule.
  - Arranging data protection training and advice for the people covered by this policy.
  - Handling data protection questions from staff and anyone else covered by this policy.
  - Dealing with requests from individuals to see the data WPIA holds about them (also called 'subject access requests').
  - Checking and approving any contracts or agreements with third parties that MAY handle the organisation's sensitive data.

- The IT manager is responsible for:
  - Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
  - Performing regular checks and scans to ensure security hardware and software is functioning properly.
  - Evaluating any third-party services the organisation is considering using to store or process data. For instance, cloud computing services.

- The marketing manager is responsible for:
  - Approving any data protection statements attached to communications such as emails and letters.
  - Addressing any data protection queries from journalists or media outlets like newspapers.
  - Where necessary, working with other staff to ensure marketing initiatives abide by data protection principles.

5.4 General staff guidelines

- The only people able to access data covered by this policy SHOULD be those who **need it for their work**.
- Data **SHOULD NOT be shared informally**. When access to confidential information is required, employees can request it from their line managers.
- **WPIA will provide training** to all employees to help them understand their responsibilities when handling data.
- Employees SHOULD keep all data secure, by taking sensible precautions and following the guidelines below.
- In particular, **strong passwords MUST be used** and they SHOULD never be shared.
- Personal data **SHOULD NOT be disclosed** to unauthorised people, either within the organisation or externally.

- Data SHOULD be **regularly reviewed and updated** if it is found to be out of date. If no longer required, it SHOULD be deleted and disposed of.
- Employees **SHOULD request help** from their line manager or the data protection officer if they are unsure about any aspect of data protection.

5.5 Data storage

These rules describe how and where data SHOULD be safely stored. Questions about storing data safely can be directed to the IT manager or data controller.

When data is **stored on paper**, it SHOULD be kept in a secure place where unauthorised people cannot see it.

These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:

- When not required, the paper or files SHOULD be kept in a **locked drawer or filing cabinet**.
- Employees SHOULD make sure paper and printouts are **not left where unauthorised people could see them**, like on a printer.
- **Data printouts SHOULD be shredded** and disposed of securely when no longer required.

When data is **stored electronically**, it MUST be protected from unauthorised access, accidental deletion and malicious hacking attempts. Especially, without limitation:

- Data SHOULD be **protected by strong passwords** that are changed regularly and never shared between employees.
- If data is **stored on removable media** (like a CD or DVD), these SHOULD be kept locked away securely when not being used.
- Data SHOULD only be stored on **designated drives and servers**, and SHOULD only be uploaded to an **approved cloud computing services**.
- Servers containing personal data SHOULD be **sited in a secure location**, away from general office space.
- Data SHOULD be **backed up frequently**. Those backups SHOULD be tested regularly, in line with the organisation's standard backup procedures.
- Data SHOULD **never be saved directly** to laptops or other mobile devices like tablets or smart phones.
- All servers and computers containing data SHOULD be protected by approved security software and a firewall.
- ...

5.6 Data use

Personal data is of no value to WPIA unless the business can make use of it. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft:

- When working with personal data, employees SHOULD ensure **the screens of their computers are always locked** when left unattended.
- Personal data SHOULD not be shared informally. In particular, it SHOULD be sent by encrypted email if any possible.
- Data MUST be **encrypted before being transferred electronically**. The IT manager can explain how to send data to authorised external contacts.
- Personal data SHOULD **never be transferred outside of the European Economic Area**.
- Employees **SHOULD NOT save copies of personal data to their own computers**. Always access and update the central copy of any data.

5.7 Data accuracy

The law requires WPIA to take reasonable steps to ensure data is kept accurate and up to date.

The more important it is that the personal data is accurate, the greater the effort WPIA SHOULD put into ensuring its accuracy.

It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

- Data will be held in **as few places as necessary**. Staff SHOULD NOT create any unnecessary additional data sets.
- Staff SHOULD **take every opportunity to ensure data is updated**. For instance, by confirming a customer's details when they call.
- WPIA will make it **easy for data subjects to update the information** WPIA holds about them. For instance, via the organisation website.
- Data SHOULD be **updated as inaccuracies are discovered**. For instance, if a customer can no longer be reached on their stored telephone number, it SHOULD be removed from the database.
- It is the marketing manager's responsibility to ensure **marketing databases are checked against industry suppression files** every six months.

5.8 Subject access requests

All individuals who are the subject of personal data held by WPIA are entitled to:

- Ask **what information** the organisation holds about them and why.
- Ask **how to gain access** to it.
- Be informed **how to keep it up to date**.
- Be informed how the organisation is **meeting its data protection obligations**. If an individual contacts the organisation requesting this information, this is called a subject access request.

Subject access requests from individuals SHOULD be made by email, addressed to the data controller at privacy (at) wpia.club. The data controller can supply a standard request form, although individuals do not have to use this.

Each person concerned will not be charged for the first request per calendar year, each following request MAY be charged with a fee of 10 EUR each.

The data controller will always verify the identity of anyone making a subject access request before handing over any information. Preferred method is a signed email or signed pdf with an advanced signature of TERACARA, alternatively an signed email or signed pdf with an qualified signature. Alternately a Verification MAY be made and the RA Agent informs the data controller about the verification. The last fallback is a registered mail to the last known postal address.

5.9 Disclosing data for other reasons

In certain circumstances, the GDPR allows personal data to be disclosed to law-enforcement agencies without the consent of the data subject (see GDPR Art. 23(1) restrictions).

Under these circumstances, WPIA will disclose requested data. However, the data controller will ensure the request is legitimate, seeking assistance from the board and from the organisation's arbitration or as last fallback from the organisation's legal advisors where necessary.

5.10 Providing information

WPIA aims to ensure that individuals are aware that their data is being processed, and that they understand:

- How the data is being used
- How to exercise their rights

To these ends, the organisation has a privacy statement, setting out how data relating to individuals is used by the organisation. This is available on request. A version of this statement is also available on the organisation's website.

6 Glossary

Glossary provided by EUROPEAN DATA PROTECTION SUPERVISOR

7 Related Documents

[^1] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG

Information nach Art. 13 für Mitglieder

Information nach Art. 13 für Fellowship

Information nach Art. 13 für Ehrenamtliche und Funktionäre