|  |
| --- |
|  |
|  |
| **DATA PRIVACY POLICY** |
|  |
|  |
| This policy defines the data privacy policy for [name] which defines our roles and responsibilities in our capacity as a data [controller] / [processor] of personal data records. |
|  |



­­­

­­­

[INTRODUCTION 3](#_Toc119400030)

[DATA PRIVACY AND PROTECTION PRINCIPLES 3](#_Toc119400031)

[GENERAL PROVISIONS 4](#_Toc119400032)

[LAWFUL, FAIR AND TRANSPARENT PROCESSING 4](#_Toc119400033)

[LAWFUL PURPOSES 4](#_Toc119400034)

[DATA MINIMISATION 5](#_Toc119400035)

[ACCURACY 5](#_Toc119400036)

[ARCHIVING / REMOVAL 5](#_Toc119400037)

[SECURITY 5](#_Toc119400038)

[DATA BREACH NOTIFICATIONS 6](#_Toc119400039)

[ARBITRATION 6](#_Toc119400040)

[PERSONAL DATA EXAMPLES (TABLE) 6](#_Toc119400041)

[EXTERNAL LINKS 7](#_Toc119400042)

[NATIONAL DATA PROTECTION SUPERVISORY AUTHORITIES 7](#_Toc119400043)

# INTRODUCTION

The General Data Protection Regulation [GDPR] enacted in May 2018 includes a series of data protection rights which you should be aware of while using our site and services. These rights are captured in principles or articles which for the purposes of this data privacy policy constitute data subject (your) rights. The next sections of our policy outline your rights in the context of GDPR and national data protection laws.

# DATA PRIVACY AND PROTECTION PRINCIPLES

We are committed to processing your data in accordance with principles outlined in Article 5 of GDPR. These principles aver that we must take due care with your data and limit our use to what's necessary for collection and retention. The full text of article 5 principles can be viewed by clicking on the button below.

|  |  |
| --- | --- |
| 1. | Data we collect must be processed lawfully, fairly and in a transparent manner in relation to individuals |
| 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 not be considered to be incompatible with the initial purposes |
| 3. | Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed |
| 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 |
| 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 subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and 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.” |

# GENERAL PROVISIONS

|  |  |
| --- | --- |
| 1. | This policy applies to all personal data [[PII]](https://gdpr.eu/eu-gdpr-personal-data/) held by us and on our behalf by [Data Processors](https://ico.org.uk/media/for-organisations/documents/1546/data-controllers-and-data-processors-dp-guidance.pdf). |
| 2. | Our Data Protection Officer shall take responsibility for our ongoing compliance with this policy |
| 3. | This policy shall be reviewed at least annually |
| 4. | We are registered with [Data Protection Authority name] as an organization that processes personal data. |

# LAWFUL, FAIR AND TRANSPARENT PROCESSING

|  |  |
| --- | --- |
| 1. | To ensure processing of your data is lawful, fair and transparent, we maintain a ["Record of Processing Activities"](https://data-privacy.io/download/7344/?tmstv=1668501708) ROPA |
| 2. | The ROPA shall be maintained on an ongoing basis as required |
| 3. | Individuals have the right to access their personal data free of charge in an accessible electronic format |
| 4. | Such requests, known as [Data Subject Access Requests](https://ico.org.uk/your-data-matters/your-right-to-get-copies-of-your-data/preparing-and-submitting-your-subject-access-request/) (DSAR’s) made to us shall be provided within 28 days (\*exceptions may apply). |

# LAWFUL PURPOSES

|  |  |
| --- | --- |
| 1. | As required by [GDPR/CCPA] all data processed by us is conducted on lawful basis. This basis includes the following four categories; Consent, Contract, Legal Obligation & Legitimate Interests ([see here for sample guidance](https://www.dataprotection.ie/en/individuals)) |
| 2. | This lawful basis is recorded in our ROPA |
| 3. | Where consent is relied upon as a lawful basis for processing data, evidence of opt-in consent shall be kept with the personal data |
| 4. | Where communications are sent to individuals based on their consent, the option for the individual to revoke their consent will be clearly available and systems will be in place to ensure such revocation is reflected accurately on our systems. |

# DATA MINIMISATION

|  |  |
| --- | --- |
| 1. | We shall ensure that personal data processing safeguards are adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed |
| 2. | Data minimisation techniques such as anonymisation will be used where possible. This is in line with our [Privacy by Design (PbD) and default](https://iapp.org/resources/article/privacy-by-design-the-7-foundational-principles/) approach to data privacy in our technology and processes. |

# ACCURACY

|  |  |
| --- | --- |
| 1. | We shall take reasonable steps to ensure personal data is accurate |
| 2. | Where necessary for the lawful basis on which data is processed, steps shall be put in place to ensure that personal data is kept up to date by all reasonable means. |

# ARCHIVING / REMOVAL

|  |  |
| --- | --- |
| 1. | To ensure that personal data is kept for no longer than necessary, we have put in place a data retention policy which covers personal data and its retention period |
| 2. | The retention policy specifies what personal data is retained, for how long and why. |

# SECURITY

|  |  |
| --- | --- |
| 1. | We shall ensure that personal data is stored and transmitted on our systems using up to date encryption methods |
| 2. | Access to personal data shall be limited to personnel who are authorized to access it for only as long as required |
| 3. | Two factor authentication and strong passwords will be used (where possible) to access systems that hold personal data |
| 4.  5.  6. | Data shall be disposed of using only approved physical and software destruction methods  Data shall be backed up using approved storage methods with strong encryption in place  Employees are trained regularly on data privacy and security risks as part of our ongoing commitment to data security. |

# DATA BREACH NOTIFICATIONS

In the event of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data, We shall promptly assess the risk to your data and if appropriate report this breach to the [data protection authority]   
In instances where a breach is likely to result in a high risk to you personally, we will inform you within 72 hours as required by the breach notification rules.

# ARBITRATION

In the event that you believe that we have not fully complied with data protection obligations with respect to your data, you retain the right to contact the data protection authority and file a complaint. This procedure can be found on [Your Data Protection Authority Homepage]

Article 9 of GDPR further defines a subset of personal data as special category or sensitive personal data which includes data subject’s racial or ethnic origin, trade union membership, physical or mental health condition or sexual life, religious beliefs and the commission or alleged commission of any offence or related proceedings.

# CONTACT INFORMATION

Our Data Protection Officer is [name] whose email address is [[email](mailto:xyz@xyz.com) address] and whose address is [address].

# PERSONAL DATA EXAMPLES (TABLE)

|  |  |
| --- | --- |
| PII (Personally Identifiable Information) | SENSITIVE PII |
| Full Name | Gender |
| Address  Date of Birth  Bank Acct no  Credit Card no | Trade Union Membership  Religion  Genetic Data  Biometric Data |
| PPS/SSN/NI No  Passport No  Driver’s License No  CCTV / Audio Footage | Sexual Orientation  Health Information  Political Opinions |
| IP Address |  |
| Cookies |  |

# FOR YOUR REFERENCE

# EXTERNAL LINKS

European Court of Justice Press Releases   
[European Court of Justice](https://curia.europa.eu/jcms/jcms/Jo2_7052/en/?types=com.jalios.jcms.Content&typesOff=generated.RecueilPublication&textSearch=true&catName=true&searchInFiles=true&langs=user&text=91%252F2017&opSearch=Search&csrftoken=eXybyksLgNzoleK0&jsp=plugins%252FCuriaPlugin%252Fjsp%252Fquery.jsp)

The 7 Principles of Privacy by Design  
<https://iapp.org/resources/article/privacy-by-design-the-7-foundational-principles/>

Data Protection and Privacy Law for Developers  
<http://www.codeproject.com/Articles/700324/Data-protection-and-privacy-law-for-developers>

Role Definition for a Data Protection Officer  
<http://www.eudataprotectionlaw.com/data-protection-officer/>

|  |  |
| --- | --- |
| NATIONAL DATA PROTECTION SUPERVISORY AUTHORITIES | |
| Austria | [http://www.dsb.gv.at](http://www.dsb.gv.at/) |
| Belgium | <http://www.privacy.fgov.be/> |
| Bulgaria | [http://www.cpdp.bg](http://www.cpdp.bg/) |
| Croatia | <http://www.azop.hr/cpage.aspx?page=default.aspx&PageID=47> |
| Cyprus | <http://www.dataprotection.gov.cy/> |
| Czech Republic | <http://www.uoou.cz/> |
| Denmark | <http://www.datatilsynet.dk/> |
| Estonia | [http://www.dp.gov.ee](http://www.dp.gov.ee/) |
| Finland | <http://www.tietosuoja.fi/> |
| France | <http://www.cnil.fr/> |
| Germany | <http://www.bfd.bund.de/> |
| Greece | <http://www.dpa.gr/> |
| Hungary | <http://abiweb.obh.hu/dpc/> |
| Ireland | <http://www.dataprotection.ie/> |
| Italy | <http://www.garanteprivacy.it/> |
| Latvia | <http://www.dvi.gov.lv/> |
| Lithuania | <http://www.ada.lt/> |
| Luxembourg | <http://www.cnpd.lu/> |
| Malta | <http://www.dataprotection.gov.mt/> |
| Netherlands | <http://www.cbpweb.nl/> |
| Poland ­ | <http://www.giodo.gov.pl/> |
| Portugal | <http://www.cnpd.pt/> |
| Romania | [http://www.dataprotection.ro](http://www.dataprotection.ro/) |
| Slovakia | <http://www.dataprotection.gov.sk/> |
| Slovenia | [http://www.ip-rs.si](http://www.ip-rs.si/) |
| Spain | <http://www.agpd.es/> |
| Sweden | <http://www.datainspektionen.se/> |
| United Kingdom | [http://www.ico.org.uk](http://www.ico.org.uk/) |
| United States | [ADPPA (Draft Legislation for International Xfers)](https://www.commerce.senate.gov/services/files/9BA7EF5C-7554-4DF2-AD05-AD940E2B3E50) [FTC (Federal Trade Commission: Bureau of Consumer Protection)](https://www.ftc.gov/about-ftc/bureaus-offices/bureau-consumer-protection) [California OAG](https://oag.ca.gov/privacy) (Office of Attorney General) [Connecticut OAG](https://portal.ct.gov/AG/Sections/Privacy/The-Privacy-and-Data-Security-Section) [NY OAG](https://ag.ny.gov/press-release/2019/attorney-general-james-statement-shield-act) |

|  |
| --- |
| [Figure 1: Visit Our Shop](https://data-privacy.io/shop) |

# USAGE NOTES

* Items in square brackets are variables, do ctrl + find to search and replace terms as necessary.
* Use the reference section to find your data protection authority
* Note that there are some variances with US privacy law and GDPR such as explicit opt-in required by GDPR vs ability to opt-out provided by CCPA
* Data protection acts at the country level may add more specificity in certain areas such as age of consent to personal data use. Reference these laws in your jurisdiction if you want to add extra detail to this policy
* If you have questions, you can reach us at [info@data-privacy.io](mailto:info@data-privacy.io?subject=Data%20Privacy%20Policy%20Question)