



General Data Protection Policy

Version Number	2	Date Reviewed and Approved	01.03.24 Reviewed and updated by Yvonne Mckeown, BHConsulting Approved by : Board Date: 21/03/2024
Review Cycle	2 years	Next Review Date	22/03/2026
Policy Area	Information	Responsible Dept.	Administration

1 General Purpose

The objective of this Data Protection Policy is to set out the requirements of Exchange House Ireland National Travellers Service (EHINTS) relating to the protection of personal data where we act as a Data Controller and / or Data Processor, and the measures we will take to protect the rights of data subjects, in line with EU and Irish legislation.

- EHINTS must comply with all applicable data protection, privacy and security laws and regulations.
- Through maintaining a high standard of data protection EHINTS wants to foster a culture that is honest, compassionate, transparent and accountable.
- In the course of our work, we are required to collect and use certain types of information about people (hereafter referred to as data subjects in line with the regulation), including 'personal data' as defined by the General Data Protection Regulation (GDPR).
- This information can relate to service users, current, past and prospective employees, suppliers and others with whom staff communicate.

2. Scope

This policy applies to all staff, students, interns and work experience candidates, contractors, sub-contractors, agency staff and authorised third party commercial service providers and other persons or entities when receiving, handling or processing personal data as defined by the GDPR.

- This policy applies to all forms of data including computer, manual and CCTV records relating to citizens.

3. Policy

It is the policy of EHINTS that all data is processed and controlled in line with the principles of the GDPR and relevant Irish legislation.

4. Data Protection Principles

The following data protection requirements apply to all instances where personal data is stored, transmitted, processed or otherwise handled, regardless of geographic location.

EHINTS will comply with the following high level principles:

- Personal data shall only be processed fairly, lawfully and in a transparent manner (Principles of Lawfulness, Fairness and Transparency);
- Personal data shall be obtained only for specified, explicit, lawful, and legitimate purposes, and shall not be further processed in any manner incompatible with those purposes (Principle of Purpose Limitation);
- Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (Principle of Data Minimisation);
- Personal data shall be accurate, and where necessary kept up to date (Principle of Accuracy);
- Personal data shall not be kept for longer than is necessary for the purposes for which the personal data are processed (Principle of Data Storage Limitation); Personal data will be retained in line with the EHINTS data retention policies.
- Personal data shall be processed in a secure manner, which includes having appropriate technical and organisational measures in place to:
 - (i) prevent and / or identify unauthorised or unlawful access to, or processing of, personal data; and
 - (ii) prevent accidental loss or destruction of, or damage to, personal data (Principles of Integrity and Confidentiality)

EHINTS shall be responsible for, and be able to demonstrate compliance with, these key principles. (Principle of Accountability)

In addition, EHINTS will ensure that data subject's rights are protected as set out in the GDPR.

Data subjects will be able to request access to data we hold on them through a Subject Access Request (SAR) (Right of Access);

- Data subjects can request to change or correct any inaccurate data (Right to Rectification);
- Data subjects have the right to object to having their data processed (Right to Restriction of Processing);
- Data subjects can request to delete data that we hold excluding medical records (Right to Erasure (sometimes referred to as the Right to be Forgotten));
- Data subjects can request to have their data moved outside of EHINTS if it is in an electronic format (Right to Data Portability);
- Data subjects can object to a decision made by automated processing, with certain limited exceptions (such as legitimate grounds for the processing or the defence of legal claims) and request that any decision made by automated processes have some human element (Right to Object to Automated Decision Making, including Profiling).

5. Data Processing Policy Requirements

EHINTS, as a Data Controller, shall be responsible for, and be able to demonstrate compliance with these GDPR Requirements.

- We will process personal data in accordance with the rights of data subjects.
- We will communicate with data subjects in a concise, transparent, intelligible and easily accessible form, using clear language.
- We will only transfer personal data to Third Parties within Ireland and outside of the European Economic Area (EEA) in accordance with this policy.

- We shall conduct all personal data processing in accordance with legitimate GDPR based processing conditions in particular;
- Data subject consent for one or more specific purposes not covered under the processing of special categories of personal data.

or

- Necessary processing for contract performance or contract entry.

or

- Legal obligation underpinning processing.

6. Processing of Special Categories of Personal Data

Special categories of data are defined by the GDPR and include data such as racial or ethnic origin, religious or philosophical beliefs, genetic data, biometric data, health data, sex life details and sexual orientation.

6.1 The processing of special categories of personal data shall be lawful where it is necessary

- for the purposes of preventative or occupational medicine,
- for the assessment of the working capacity of an employee,
- for medical diagnosis,
- for the provision of medical care, treatment or social care,
- for the management of health or social care systems and services, or
- pursuant to a contract with a health professional.

6.2 Processing is lawful where it is undertaken by or under the responsibility of

- a health practitioner, or
- a person who in the circumstances owes a duty of confidentiality to the data subject that is equivalent to that which would exist if that person were a health practitioner. For example the outpatient clinic secretary, Emergency Department Receptionist, Primary Care Centre Staff etc.
- If the processing of data is not covered by the categories above EHINTS will require explicit consent from the data subject.

6.3 Processing of Personal Data

- The processing is necessary in order to protect the vital interests of the person (referred to as the data subject in Data Protection language). This would apply in emergency situations such as in the Emergency Department when unconscious, sharing information with other emergency services for rescue or relocation in storms etc.
- The processing is necessary for a task carried out in the public interest or in the exercise of official authority vested in EHINTS.
- Processing of personal data is permitted where is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.

6.4 Data Storage Limitation Policy

EHINTS should erase any personal data that violates;

- Data Protection Law
- Data Protection Regulations
- Contractual Obligations
- Requirements of this Policy

- If EHINTS no longer requires the Data

6.5 Data Anonymisation and Pseudonymisation

EHINTS must anonymise and / or pseudonymise personal data when it is being used for purposes other than the direct provision of public health and health and social care services.

6.6 Information Security

All EHINTS staff must familiarise themselves with the up to date information security policies.

7. Unauthorised Disclosure

- All persons covered under this policy are prohibited from disclosing a data subject's confidential information (including personal data or special categories of personal data), unless this policy or a legal basis allows for such disclosures.
- All persons covered under this policy must report all suspected incidents of unauthorised access to the relevant deputy Data Protection Officer (DPO). Incidents include disclosure, loss, destruction or alteration of patient and service user's personal information, regardless of whether it is in paper or electronic form.
- EHINTS has established formal procedures for reporting suspected incidents of unauthorised disclosure of data. All persons covered under this policy must follow these procedures.

8. Privacy by Design, Data Protection by Design & Data Protection by Default Policy

EHINTS aims to use its systems and processes which are guided by strict adherence to data protection legislation in the delivery of health and social care services.

Aside from general data protection policy we must incorporate the following principles in projects involving the design of a new or changing an existing service.

- Privacy by Design and by Default
- Data Protection by Design and by Default

If any staff member considers that particular class of personal data processing may affect a data subject's rights and freedoms then they should;

- Engage the DPO or deputy DPO in terms of the issue.
- Conduct a mandatory Data Protection Impact Assessment (DPIA).
- All Data Protection Impact Assessments must be registered with the DPO office.

9. Third Party Transfer Policy

- EHINTS must not transfer personal data to a Third Party outside of the EEA regardless of whether EHINTS is acting as a Data Controller or Data Processor unless:
- The EU recognises the transfer country/territory as having an adequate level of data subject legal protection relating to personal data processing or
- The EU recognises the transfer mechanism as providing adequate protection when made to countries/territories lacking adequate legal protection.
- The explicit consent of the data subject is required to allow Third Party transfer or transfer is authorised by law.
- All reasonable, appropriate and necessary steps have been taken to maintain the required level of Personal data Protection; and

- Subject to the provisions above, including any necessary EHINTS approvals, EHINTS may transfer personal data to a Third Party outside of the EEA where any of the following apply:
 - The transfer is necessary to protect the data subject's vital interests; or
 - The data subject has given explicit consent to the proposed transfer; or
 - The transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between EHINTS and a Third Party; or
 - The transfer is necessary or legally required for the establishment, exercise, or defence of legal claims; or
 - The transfer is required by law; or
 - The transfer is made from a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest.
 - The DPO must assess whether any of the above exceptions apply prior to any personal data transfer and must record the determination in writing.

10. Third Parties Relationships Policy

- Where EHINTS engages a Third Party for processing activities, this Data Processor must protect personal data through sufficient technical and organisational security measures and take all reasonable GDPR compliance steps.
- When engaging a Third Party for personal data processing, EHINTS must enter into a written contract, or equivalent. This contract or equivalent shall:
 - Clearly set out respective parties responsibilities
 - Must ensure compliance with relevant European and local Member State Data Protection requirements/legislation.
 - At the expiry of a data processor contract the data processor is contractually obliged to return the full dataset to EHINTS and provide unequivocal evidence that their copy of the dataset is erased.
 - EHINTS must ensure that all Third Party relationships are established and maintained. Data processors who are processing data on behalf of EHINTS must secure approval from EHINTS if they wish to engage further data processors

11. Education and Awareness Policy

- EHINTS will ensure that staff receive General Data Protection Regulation training staff may receive additional training when applicable to their duties or position.

12. Roles and Responsibilities

12.1 Office of the Data Protection Officer

- The data protection officer (DPO) and deputy data protection officers should be involved, properly and in a timely manner, in all issues which relate to the protection of personal data. They are bound by secrecy or confidentiality concerning the performance of their tasks, in accordance with Union or Member State law.
- They are responsible for monitoring compliance with the GDPR and have overall control of how data is processed within EHINTS.
- This will include:
 - Collecting information about processing activities
 - Analysing and checking the compliance of processing activities,

- Informing, advising and issuing recommendations management and the relevant data processors and controllers
- Where a national unified or coordinated response is needed, cooperation/collaboration with other organisations DPOs may take place.

12.2 Enforcement

- EHINTS reserves the right to take such action as it deems appropriate against individuals who breach the conditions of this policy. EHINTS staff who breach this policy may be subject to disciplinary action as provided for in EHINTS disciplinary procedure. If a breach occurs due to reckless behaviour and a breach occurs and is knowingly not reported, the person responsible may be held accountable.
- Where a breach of this policy is committed by contractors, sub-contractors, agency staff and authorised third party commercial service providers, EHINTS reserves the right to remedy via the contracts in existence.

12.3 Data Breach Notification

All personal data breaches must be reported immediately to EHINTS Contact. This includes personal data breaches which relate to personal data being handled by employees, agents, contractors, or other parties working on behalf of EHINTS from home.

If a personal data breach occurs and that breach is likely to result in a risk to the rights and freedoms of data subjects (e.g. financial loss, breach of confidentiality, discrimination, reputational damage, or other significant social or economic damage), the Data Protection Contact must ensure that the relevant Supervisory Authority is informed of the breach without delay, and in any event, within 72 hours after having become aware of it.

In the event that a personal data breach is likely to result in a high risk to the rights and freedoms of data subjects, the Data Protection Contact must ensure that all affected data subjects are informed of the breach directly and without undue delay.

Data breach notifications shall include the following information:

- The categories and approximate number of data subjects concerned.
- The categories and approximate number of personal data records concerned.
- The name and contact details of ARC Cancer Support data protection contact (or another contact point where more information can be obtained);
- The likely consequences of the breach.
- Details of the measures taken, or proposed to be taken, by ARC Cancer Support to address the breach including, where appropriate, measures to mitigate its possible adverse effects.

12.4 Review & Update

- This policy will be reviewed and updated every 3 years or more frequently if necessary to ensure any changes to EHINTS's organisation structure and business practices are properly reflected in the policy.

Glossary of Terms

Anonymised Means the process of making personal data anonymous data. 'Anonymise' should be construed accordingly.

Anonymous Data means any information relating to a natural person where the person cannot be identified, whether by the Data Controller or by any other person, taking account of all the means reasonably likely to be used either by the Data Controller or by any other person to identify that individual.

Biometric Data means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data

Consent means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

Data as used in this Policy shall mean information which either:

- is processed by means of equipment operating automatically in response to instructions given for that purpose;
- is recorded with the intention that it should be processed by means of such equipment;
- is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system;
- Does not fall within any of the above, but forms part of a readily accessible record.
- Data therefore includes any digital data transferred by computer or automated equipment, and any manual information which is part of a relevant filing system.

Data Controller means a person or organisation who (alone or with others) determines the purposes for which and the manner in which any personal data are, or are to be, processed. A Data Controller can be the sole Data Controller or a joint Data Controller with another person or organisation.

Data Processor means a person or organisation that holds or processes personal data on the instructions of the Data Controller, but does not exercise responsibility for, or control over the personal data.

Data Protection means the protection of personal data

Data Protection Commission means the office of the Data Protection Commission in Ireland.

Data subject refers to the individual, to whom personal data held relates, including: employees, customers, suppliers.

DPO Data Protection Officer