

IronOak



IRON OAK

**GDPR POLICY & COMPLAINTS
PROCEDURE**

Control Sheet

Version number	03
Date approved by Board	24 July 2026
Date of next review	June 2027
Status	Published
Policy owner	Data Protection Officer (DPO)
Policy location	IronOak Shared Drive/BrightHR
Target group	Employees

Document History:			
Version	Date of review	Author	Note of revisions
02	June 2026	DPO	- Reformatted to meet the requirements of Management of Policies Policy. - Amendment to the guidance adopted regarding file retention. - Addition of the complaints procedure

Excellence ➤ Safety ➤ Sustainability ➤ Integrity

1. Introduction

- 1.1. IronOak Homes (IronOak) is registered as a society under the Co-operative and Community Societies Act 2014. IronOak is a non to profit organisation and nothing shall be paid or transferred by way of profit to Shareholders of the Society.
- 1.2. The aim of this policy is a statement that sets out how this organisation protects personal data. It is based on a set of principles, rules and guidelines that informs you how we will ensure ongoing compliance with data protection laws. It explains the general data protection regime that applies to most UK businesses and organisations. It covers the UK General Data Protection Regulation (UK GDPR), tailored by the Data Protection Act 2018.
- 1.3. As an organisation handling personal data (including sensitive data) on a day to day basis, this policy sets out the requirements of the Act and how we, as an organisation will meet our legal obligations. Staff awareness and understanding of their responsibilities regarding the handling, collection and retention of data will be core to the successful embedding of this policy.
 - Responsibility for ensuring data protection compliance falls to the executive board and senior management team.
 - This policy is written and overseen by the Data Protection Officer
 - All staff (including temporary staff, casual staff, volunteers, apprentices and work experience) must comply with this policy. Managers have a duty to ensure staff have read this policy before starting to process any personal data.
 - All staff have a duty to report a breach of this policy to the Data Protection Officer
 - Data Processors (contractors, suppliers and sub-contractors) and joint controllers or partners, will have contractual terms drawn up based on this policy to ensure a level of compliance with it, ensuring they manage data in a transparent, appropriate, secure and legal manner
- 1.4. This document includes the procedure for raising complaints relating to the processing of personal data in accordance with:
 - UK GDPR;
 - Data Protection Act 2018;
 - applicable UK data protection legislation;
 - the requirements introduced under the Data (Use and Access) Act 2025.
- 1.5. IronOak is committed to handling complaints fairly, consistently, and without undue delay.
- 1.6. Where relevant this policy will incorporate detailed guidance and statutory code of practice from the Information commissioner's office (ICO) as the UK's independent body which was set up to uphold information rights and regulate data protection in the UK.

Excellence ➤ Safety ➤ Sustainability ➤ Integrity

2. Purpose

2.1. The Data Protection Act 2018 UK General Data Protection Regulation (UK GDPR) sets standards for protecting personal data and gives people more control over the use of their data.

- There are 4 main matters provided for, these are:
- General Data Processing
- Law Enforcement Data processing
- Data Processing for National Security Purposes
- Enforcement

2.2. All the above need to be set in the context of international, national, and local data processing systems which are increasingly dependent upon internet usage for the exchange and transit of data. The UK must lock into international data protection arrangements, systems, and processes, and this Act updates and reinforces the mechanism to enable this to take place.

2.3. This policy covers:

- Definitions
- UK Data Protection Principles
- Lawful bases for processing (including special categories of data and criminal convictions)
- Individual Rights
- Privacy Notices
- Privacy and Electronic Communications Regulations (PECR)
- File Retention
- Data Protection Impact Assessments (DPIAs)
- Data Processing
- Data Sharing
- Breach Management
- Data Protection Officer
- ICO and Registration
- Related Guidance
- Training Statement

3. Legislation

3.1. The UK GDPR lays out the following:

- 8 Principles for data processing.
- Specific and detailed lawful bases and legal bases for processing personal data (including special categories of data).
- Rights of Data subjects

Excellence ➤ Safety ➤ Sustainability ➤ Integrity

3.2. The below items will detail and outline these elements and explain their practical application for IronOak and any other existing policies, procedures and actions required to support them.

4. Data Protection Principles

4.1. The Act sets out 8 Principles which must be adhered to when processing data. Please refer to the Related Guidance links for further information.

4.2. The GDPR sets out the following principles for which this organisation is responsible and must meet. These require that personal data shall be:

- processed lawfully, fairly and in a transparent manner in relation to individuals
- be collected for specified, explicit and legitimate purposes, and not further processed in a manner that is incompatible with 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 adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
- accurate and where necessary, kept up to date, every reasonable step must be taken that personal data that is inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay
- 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 purposes in so far 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 the appropriate technical and organisational measures required by the GDPR (the safeguards) in order to safeguard the rights and freedoms of individuals
- 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

4.3. "The controller shall be responsible for, and be able to demonstrate, compliance with the principles" Article 5 (2) GDPR.

5. The Lawful basis for processing Personal Data

5.1. Personal data shall only be processed if one of the following legal basis can be met:

- The Data Subject has given consent to the processing of their data; or
- The processing is necessary for a contract the Data Subject is party to, or in order to take steps prior to entering into a contract (e.g. a Tenancy Agreement, or applying for a tenancy); or

Excellence ➤ Safety ➤ Sustainability ➤ Integrity

- The processing is necessary for compliance with a legal obligation to which IronOak is subject; or
- The processing is necessary to protect the vital interests of the data subject or another natural person; or
- The processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; or
- The processing is necessary for the purposes of a legitimate interest of the Data Controller or by a third party except where such interests are overridden by the interests or rights and freedoms of the Data Subject, in particular where the Data Subject is a child.

5.2. Where possible, IronOak will refrain from using 'consent' as a basis to process data due to its 'right to withdraw' which could affect our ability to provide and deliver our services.

5.3. When using 'Legitimate interests' as a base for processing, the organisation must ensure they complete a PIA/DPIA (impact assessment) which outlines risks and ways in which risks will be reduced to ensure the rights and freedoms of the affected data subjects are protected.

5.4. NOTE: If and when relying on consent the following must apply:

- Consent must be demonstrable;
- Consent in the form of a written declaration must be distinguishable from other matters, and requested in an intelligible and easily accessible form, using clear and plain language;
- The Data Subject may withdraw consent at any time, and withdrawal must be as easy as giving consent; (when processing data of Children under 16 years old, Consent to process should be sought from a Parent or Guardian, with exception of 'online services' delivered to the child, where the age of consent is 13 according to UK law).

6. Legal basis for processing Special Categories of Data

6.1. In order to process Special Categories of Personal Data (see Definitions for clarification) one or more of the additional grounds below must also be met:

- The Data Subject has given explicit consent for the processing for specific purposes; or
- For employment, social security and social protection law processes, as set out in EU and UK law and providing appropriate safeguards for the rights and freedoms of subjects are in place; or
- To protect the vital interests of Data Subjects or another natural person where the Subject is physically or legally incapable of giving consent; or
- Processing carried out as part of the legitimate activities of a non-for-profit organisation with a political, philosophical, religious or trade union aim, where

Excellence ➤ Safety ➤ Sustainability ➤ Integrity

the processing is solely for members or former members of the body or to persons who have regular contact with it in connection to its purposes and that the personal data is not disclosed outside that body without the subject consent; or

- Processing related to personal data made public by the subject; or
- Processing necessary for the establishment, exercise or defence of a legal claim or for courts acting in a judicial capacity; or
- Processing is necessary for the purpose of substantial public interest, on the basis of EU and UK Law which will be proportionate to the aim pursued, respect the essence of the Data Protection rights and provide for suitable and specific safeguarding measures to the rights and interests of the subject; or
- Processing is necessary for preventative or occupational medicine, the assessment of the working capacity of employees, medical diagnosis, provision of health or social care or treatment or the management of health or social care services based on state law or pursuant of a contract with a health care professional; or
- Processing is necessary for the reasons of public interest in relation to public health such as cross-border threats to health, ensuring high quality of health care, medical devices or medicinal products based on state law that safeguards the rights and freedoms of subjects, particularly professional secrecy; or
- Processing for archival purposes in the public interest, scientific or historical research or statistical purposes (where appropriate safeguards are in place and data is either pseudonymised or anonymised completely).

6.2. When handling Special Categories of personal data, 'explicit consent' maybe a more appropriate. The rules for consent as defined under 'personal data lawful bases' and the subsequent Note still applies.

7. Criminal Conviction Data

7.1. Criminal conviction data cannot be collected or processed unless there is a legitimate legal basis to do so or a legal authority imposed upon the organisation.

- We may process criminal data in relation to employment under the terms of the Rehabilitation of Offenders Act, in relation to specific and designated roles within the organisation, which meet the criteria set out by the Disclosure and Barring Service.
- Criminal data must be collected and processed in-line with the above principles, including being the minimum data to accomplish its purpose, updated regularly and/or disposed of once it is used for its specific purpose and kept secure – only being visible to those that require access to it.
- Criminal conviction data can be processed for other purposes, but they must be carried out under a specific legal requirement or authority bestowed upon us or an employee or must meet the substantial public interest requirements

Excellence ➤ Safety ➤ Sustainability ➤ Integrity

of the Data Protection Act 2018. When looking to process data on this basis, the process must be documented and an appropriate risk assessment carried out, preferably using a PIA and should be reviewed by the Data Protection Officer, due to the potential risks and requirement to notify the ICO of any potentially high risk processing we plan to carry out (see 'PIA' section below).

8. Individual Rights

8.1. There are several changes here in particular the Right of Access in relation to timescales and fees. These must be fully understood in relation to anyone submitting a Subject Access request. Please refer to the related Guidance Link

8.2. The UK GDPR provides the following rights for individuals:

- right to be informed
- right of access
- right to rectification
- right to erasure
- right to restrict processing
- right to data portability
- right to object
- rights in relation to automated decision making and profiling.

8.3. For any individual request which falls into the above categories, IronOak will follow the relevant guidance currently available on the following website:

<https://ico.org.uk/for-organisations>

8.4. Each of the above rights has its own Best Practice Process which you will find here:

<https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/individual-rights/individual-rights/>

9. Privacy Notices

9.1. This is a requirement for data processing, it is an accessible information declaration which should set out clearly how we will gather, use handle, store and process personal data.

9.2. The Code uses the term "Privacy Notice" to describe all the privacy information that you make available or provide to individuals when you collect information about them. It is often argued that people's expectations of personal data are changing, particularly through the use of social media, the use of mobile apps and the willingness of the public to share personal information via these platforms.

9.3. However, as an organisation we are increasingly aware of the fragile trust which can be easily broken through data breaches and are therefore seeking transparency as a means of building trust and confidence with users of our services. It is the spirit of the Act that privacy, transparency and control become a given for users.

Excellence ➤ Safety ➤ Sustainability ➤ Integrity

9.4. Being transparent by providing a privacy notice is an important part of fair processing and a privacy notice is the most common way to meet UK GDPR requirements. When planning a privacy notice, we need to consider the following:

- what information is being collected?
- who is collecting it?
- how is it collected?
- why is it being collected?
- how will it be used?
- who will it be shared with?
- what will be the effect of this on individuals concerned?
- is the intended use likely to cause individuals to object or complain?

9.5. The Privacy notice must be easily understood by users of the service and include all of the above, it must also be easily visible so in this organisation it will be displayed within the appropriate management documentation.

9.6. We use personal data (information that relates to and identifies living people) and other information to help us to carry out our role as a Housing Provider in England.

9.7. We will always make sure that your information is protected and treated securely. Any information about you that we hold, or details you give us, will be held in accordance with the Data protection law - the General Data Protection Regulation (GDPR) and the Data Protection Act 2018.

10. Privacy and Electronic Communications Regulations (PECR)

10.1. This guide issued by the ICO covers specifically electronic marketing messages i.e. phone, fax, email or text, and includes the use of cookies. It introduces specific roles on the above keeping such communication services secure and user's privacy in regard to traffic and location data, itemised billing, line identification and directory listings.

10.2. The Data Protection Act 2018 still applies if you are processing personal data. The PECR sets out some extra rules for electronic communications and please be mindful of electronic schedule systems which will also come under PECR. This will apply to the digital care planning system and the Resident record electronic system.

11. File Retention

11.1. The GDPR sets out Guidance on files and retention including archiving, specifically Health and Social Care personal data is generally exempt.

Excellence ➤ Safety ➤ Sustainability ➤ Integrity

11.2. We abide by The National Housing Federation document retention schedule, NHS England guidance and specific Local Authorities requirements documented within the Service Specification when retaining data.

11.3. A periodic check of the National Housing Federation's document retention schedule and NHS England's guidance should be part of the review of this policy.

11.4. It is the responsibility of the data owners to ensure this is carried out regularly to ensure data is not stored beyond its retention period.

12. Data Protection Impact Assessments

12.1. Where carrying out any new data collection or processing that may have a potential impact on Data Subjects, a DPIA must be completed to ensure accountability for the proposed processing and to ensure all Data Protection risks are documented and managed. The Data Protection Officer will make a template document available with guidance on how to complete this or record the appropriate information for a DPIA.

12.2. For all new internal projects, a DPIA must be completed alongside the business case.

12.3. If the piece of work or change does not flag one of the screening questions within the DPIA, the rest of the form does not need completing, but the screening questions must be recorded as showing the form is not required.

12.4. For smaller changes, a reduced format Privacy Impact Assessment (PIA) form may be completed, for expediency, but it must record how the proposed change will meet the principles of the legislation.

12.5. Where there is a discernibly high risk to individuals' data or where a large amount of special category personal data is being processed, the DPIA should be shared with the ICO, to potentially provide additional consultation or advice on how to manage the processing and ensure the upholding.

12.6. The DPIA risk map should be used to capture any data risks and produce an action plan for remedying or mitigating these risks. These should be managed by the data owner.

13. Data Processing

13.1. Personal data must always be processed in-line with the data protection principles.

13.2. Records of processing (ROPAs) must be maintained. These may be audit logs within computer systems, or as other digitally recorded logs held in another manner. These are to capture data changes and access, to ensure that any

Excellence ➤ Safety ➤ Sustainability ➤ Integrity

processing or actions that may have led or contributed to a breach can be captured and interrogated.

- 13.3. Changes to data processing, must be considered in-line with the DPIA documents and updated therein. Any changes which will have a significant impact on the rights or freedoms of subjects or involve a significant change in the amount of or nature of the data processed (such as adding special category personal data) may require a full DPIA review.
- 13.4. Appropriate risks should be logged and remedial action plans put in place, to ensure ongoing compliance.
- 13.5. DPIAs will be used as a basis for carrying out Data Protection audits on a team's compliance, ensuring processes are followed and risk mitigating elements are upheld.
- 13.6. This policy applies to all data held in relation to living, personally identifiable individuals and information processing, including collection, storage and destruction, for data held in both physical formats (i.e. paper) and digital formats (i.e. on computers, mobile devices etc.).
- 13.7. This policy does not apply to non-personal business data, but equivalent privacy, confidentiality and security measures from this policy should be applied.
- 13.8. This policy does not relate to deceased individuals. An air of confidentiality would be appropriate when disclosure of a deceased person's personal data is requested.
- 13.9. Note: When disclosing information pertaining to a deceased individual, proof of death should be sought, e.g. a death certificate, and secure identification of the requesting individual should be put in place, to facilitate disclosure to a next of kin, executor of a will or similar, (An appropriate security check should be done whenever disclosing, amending, restricting or otherwise processing data, from a direct instruction from the data subject or a representative of theirs, in a method where immediate identification is not easy. Examples of these circumstances are such as face-to-face when the individual is unknown to you; over the telephone; via email; via webchat or any other similar method of communication. This is to prevent disclosing data to anyone misrepresenting an individual and in so doing, preventing a breach incident).

14. Data Sharing and Disclosure

- 14.1. All data sharing and disclosure must be done in-line with IronOak's Data Sharing and Disclosure Procedure.

Excellence ➤ Safety ➤ Sustainability ➤ Integrity

- 14.2. An appropriate security check should be done whenever disclosing, amending, restricting or otherwise processing data, from a direct instruction from the data subject or a representative of theirs, in a method where immediate identification is not easy. Examples of these circumstances are such as face-to-face when the individual is unknown to you; over the telephone; via email; via webchat or any other similar method of communication. This is to prevent disclosing data to anyone misrepresenting an individual and in so doing, preventing a breach incident.
- 14.3. Security questions should be of a unique enough nature that they would not be publicly available and should ask for confirmation of data we possess, that is known to the data subject only. For example, data of birth, postcode, address etc. are easily and readily available to many people on public registers, whereas someone tenancy reference number, how much their rent is or how they pay for their rent would not be.
- 14.4. Each team, interacting with individuals, using methods where identification is an issue, should make specific procedures for how to manage such security identification. These may address any specific needs of their customers and the risks related to the data they process. Appropriate training should be delivered to ensure compliance with these procedures.
- 14.5. Managers have a responsibility to ensure that these security procedures are in place and are adhered to. They may do this through audits of communications.
- 14.6. Where staff are not adhering to these procedures and failing to check security, appropriate steps should be taken to address the risk of potential breach incidents
- 14.7. When sharing data with a third party, an appropriate legal gateway must be used to facilitate this, as per sections (D.P principles). Where consent is required, this must be demonstrable both for transparency to the subject and to ensure the transfer between IronOak and the recipient has a legal basis.
- 14.8. Where systematic sharing is required to a third party in relation to service provision for a customer (e.g. a carer representing a disabled resident or emergency contact), a data sharing consent form must be signed capturing information for IronOak to be able to prove the identity of the third party when the contact us.
- 14.9. Where relying on legal provisions such as a Power of Attorney, information should be gathered to ensure identification of the individual. Proof of the Power of Attorney or other legal basis should be sought to ensure the validity of the relationship.
- 14.10. Where disclosing data for the purposes of criminal investigation by the police, the data disclosed should be recorded. If the sharing is felt to be inappropriate (i.e. for 'fishing' purposes), this may be deferred back to the requesting officer, and we may request that the appropriate warrant is sought.

Excellence ➤ Safety ➤ Sustainability ➤ Integrity

14.11. When collecting data about third parties, these individuals become data subjects and should be informed as such, as per section (Data subject individual rights).

15. Information Security

15.1. Information security is essential for all types of confidential records, whether manual or electronic. We ensure staff takes basic precautions against information security breaches, such as not leaving portable computers, resident notes, or files in unattended cars or easily accessible areas.

15.2. Staff are made aware of data protection policies and procedures during their induction and receive further training on an annual and when-required basis.

15.3. Staff supervision, staff meetings, and guides clearly emphasise the importance we put on the security of personal and sensitive information that we are required to collect by our regulators.

15.4. All files and portable equipment should be stored under lock and key when not being used. Staff should not take residents' records home (unless WFH is relevant).

15.5. We use a secure Email system or equivalent for all our communications of sensitive personal data.

15.6. All staff receive training on information security management and how to share information safely.

16. Training

16.1. All staff are made aware of the organisation's policies and procedures during induction, all of which are used for training updates.

16.2. All policies and procedures are reviewed and amended where necessary and staff are made aware of any changes.

16.3. Observations are undertaken to check skills and competencies.

16.4. Various methods of training are used including one to one, e-learning, group meetings, individual supervisions and external courses are sourced as required.

17. Breach management

17.1. Data Breaches will be managed in line with the Data Breach Procedure.

17.2. Data Breaches, or potential data breaches, must be notified to the Data Protection Officer as soon as an individual in the organisation is aware of this happening or is informed by a Data Processor or Data Recipient.

Excellence ➤ Safety ➤ Sustainability ➤ Integrity

17.3. Where a breach needs to be disclosed to the ICO this must be done within 72 hours of the incident being raised, by the Data Protection Officer.

17.4. Where there is a high risk to the individual(s) affected, we must inform them, including any remedial action they need to take to additionally protect themselves.

17.5. Where a breach has occurred, the CEO must be informed.

18. Data Protection Officer (DPO)

18.1. The DPO is a mandatory requirement under Article 37 of the GDPR and is responsible for:

- Advising IronOak on all matters in relation to Data Protection and as such should be involved in any issues as soon as practicable;
- Advise on appropriate employee training/responsibility of their obligations under the Data Protection legislation;
- Advise on and implement policies and procedures for data protection tasks and duties;
- Cooperate with and act as a contact for the Information Commissioners Office.
- The DPO shall ensure compliance with the Data Protection legislation, having the protections laid out in the GDPR legislation and shall have reporting access to the highest level of management within IronOak.
- Data Subjects shall have a route(s) of direct access to the DPO to report issues, raise queries and make rights requests.
- The DPO shall be bound by secrecy and confidentiality concerning the performance of their tasks.
- The DPO shall be granted appropriate access to all data held by IronOak in accordance with carrying out their tasks, primarily in order to facilitate rights requests and audit data processing, and investigation of data breaches.

18.2. The DPO can be contacted at dpo@IronOakhomes.co.uk

19. Complaints Procedure

19.1. How to Make a Complaint

19.1.1. Individuals may submit a complaint using any of the following methods:

- Email: dpo@ironoak.org.uk
- Post: DPO, IronOak Homes, AGF House, 3-5 Rickmansworth Road, Watford, Herts, WD18 0GX
- Telephone: 01923 987333

19.1.2. Complaints should include:

- the complainant's name and contact details;

Excellence ➤ Safety ➤ Sustainability ➤ Integrity

- description of the concern;
- relevant dates;
- any supporting information or documents.

19.1.3. The organisation may request proof of identity where necessary.

19.2. Complaint Handling Principles

19.2.1. The organisation will:

- treat complaints confidentially;
- handle complaints fairly and impartially;
- investigate complaints appropriately;
- keep records of complaints;
- take corrective action where necessary;
- respond without undue delay.

19.3. Complaint Handling Process

19.3.1. Stage 1 – Receipt and Logging

19.3.1.1. Upon receipt:

- the complaint will be logged in the Data Protection Complaints Register;
- a reference number will be assigned;
- the complaint owner will be identified.

19.3.1.2. The following information should be recorded:

- complaint reference;
- date received;
- complainant details;
- nature of complaint;
- responsible investigator;
- status and outcome.

19.3.2. Stage 2 – Acknowledgement

19.3.2.1. The organisation will acknowledge receipt of the complaint within 30 days.

19.3.2.2. The acknowledgement should include:

- confirmation the complaint has been received;
- expected next steps;
- likely response times;
- contact details for further queries.

19.3.3. Stage 3 – Investigation

19.3.3.1. The investigator or Privacy Lead will:

Excellence ➤ Safety ➤ Sustainability ➤ Integrity

- review the complaint details;
- identify relevant processing activities;
- gather evidence and records;
- interview relevant staff if required;
- assess compliance with UK GDPR obligations;
- determine whether corrective action is necessary.

19.3.3.2. Where appropriate, the organisation may:

- restrict processing temporarily;
- correct inaccurate data;
- delete data;
- improve controls or procedures;
- provide additional staff training.

19.3.3.3. Complex complaints may be escalated to the DPO, legal counsel, or senior management.

19.3.4. Stage 4 – Outcome Response

19.3.4.1. A written response will be provided to the complainant including:

- summary of the complaint;
- investigation findings;
- actions taken (if applicable);
- rationale for decisions;
- information regarding escalation rights.

19.4. Escalation Rights

19.4.1. Individuals may contact the UK Information Commissioner's Office if dissatisfied with the outcome.

19.4.2. ICO Contact Details: <https://ico.org.uk/make-a-complaint/>

19.5. Complaint Timescales

19.5.1. Activity Timescale:

Activity	Timescale
Complaint acknowledgement	Within 30 days
Initial assessment	As soon as practicable
Investigation completion	Without undue delay
Outcome communication	Promptly after investigation

Excellence ➤ Safety ➤ Sustainability ➤ Integrity

19.6. Record Retention

19.6.1. Complaint records shall be retained for 6 years in accordance with the organisation's retention schedule.

19.6.2. Records may include:

- complaint correspondence;
- investigation notes;
- evidence reviewed;
- decisions made;
- remediation actions.

19.6.3. Access to complaint records shall be restricted to authorised personnel.

20. ICO & Registration

20.1. The Information Commission Office is the UK's supervising authority.

20.2. Within the Enforcement Toolbox, the Information Commissioners' Office known as the I.C.O. can now issue substantial fines of up to 20 million, or, 4% of an organisation's global turnover for certain data protection infringements. Fines, when appropriate, will be at the discretion of the I.C.O. with considerable variations expected to be levied. There are no fixed penalties or minimum fines, though there are different maximum fines for different breaches. The UK GDPR also empowers the I.C.O. to create tailor-made solutions to deal with infringements brought to their attention. This does not mean that organisations can relax about compliance, but diligent small and medium-sized organisations can take comfort in the fact that they are unlikely to face the sort of punitive fines that rogue tech giants could face.

20.3. The highest imposed fine limit was £500,000 under the old Act (1998) but the highest fine ever imposed was £400,000 to TalkTalk for failings in connection with a cyber-attack in 2016. The Information Commissioner is playing down the "scaremongering because of misconceptions". £20 million fines could put businesses out of business and that is not the intention of the UK GDPR, though there is a seismic shift in the number of fines that could be imposed.

20.4. The role and scope of the I.C.O. have not fundamentally changed but rather have been expanded and enhanced via the UK GDPR.

20.5. IronOak is registered with the ICO, logging all required information, including the details of the DPO. This is renewed annually, on the anniversary of the original registration. The registration references are: IronOak Homes. Reg No: ZB316753.

20.6. IronOak will, via the DPO, ensure an open relationship with the ICO, referring to them for advice, recording relevant DPIAs and logging any breach incidents which meet the reporting requirements from the legislation.

Excellence ➤ Safety ➤ Sustainability ➤ Integrity

21. Related Guidance

- Smaller Organisations ICO <https://ico.org.uk/for-organisations/business/>
- Guide to the UK General Data Protection Regulation (GDPR)
<https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf>
<https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/>
- ICO Data protection Self-Assessment <https://ico.org.uk/for-organisations/resources-and-support/data-protection-self-assessment/>
- Direct Marketing Guidance <https://ico.org.uk/media/for-organisations/documents/1555/direct-marketing-guidance.pdf>
- Data Protection Fees Information Commissioner <https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/02/new-model-announced-for-funding-the-data-protection-work-of-the-information-commissioner-s-office/>
- Example of Privacy Notice <https://www.johnlewis.com/customer-services/shopping-with-us/privacy-notice>
- Guide to privacy and Electronic Communications Regulations (PECR)
<https://ico.org.uk/for-organisations/guide-to-pecr/>
- Data Protection and the use of criminal offence data for employment and education purposes August 2018 <https://www.nacro.org.uk/wp-content/uploads/2018/08/Nacro-briefing-Data-protection-and-the-use-of-criminal-offence-data.pdf>