PRIMA GROUP

Data Protection Policy

Contents

Data Protection Policy

1 Aim of the Policy

The General Data Protection Regulation (GDPR) has been retained in UK law as the UK GDPR and will continue to be read alongside the Data Protection Act 2018 (DPA 2018), with technical amendments to ensure it can function in UK law.

- Data protection is about ensuring our customers can trust Prima to use their data fairly and responsibly.
- If Prima collects information about individuals for any reason we need to comply.
- The onus is on Prima to think about and justify how and why we use data.
- The Information Commissioner's Office (ICO) regulates data protection in the UK and offers advice and guidance, promotes good practice, carries out audits, considers complaints, monitors compliance and takes enforcement action where appropriate.

The aim of this policy is to ensure Prima Group is compliant with the UK GDPR, and the DPA 2018.

2 Who does this Policy apply to?

This policy will apply to all Prima Group employees, Board Members, Involved Residents and any other person handling data on behalf of the Group, including consultants and contractors. It outlines the responsibilities of Prima Group and its employees in respect of the collection, use and disclosure of data and the rights of the customers, employees and other parties to have access to personal data concerning them.

3 Policy Statement

The UK GDPR is the UK General Data Protection Regulation. It is a UK law which came into effect on 01 January 2021. It sets out the key principles, rights and obligations for most processing of personal data in the UK, except for law enforcement and intelligence agencies.

It is based on the EU GDPR (General Data Protection Regulation (EU) 2016/679) which applied in the UK before that date, with some changes to make it work more effectively in a UK context.

The DPA 2018 sits alongside and supplements the UK GDPR. It sets out the framework for data protection law in the UK - updates and replaces the Data Protection Act 1998 - and came into effect on 25 May 2018. It was amended on 01 January 2021 by regulations under the European Union (Withdrawal) Act 2018, to reflect the UK's status outside the European Union (EU).

On 28 June 2021, the EU approved adequacy decisions for the EU GDPR and the Law Enforcement Directive (LED). This means data can continue to flow as it did before, in the majority of circumstances. Both decisions are expected to last until 27 June 2025.

Prima occasionally processes personal data in connection with providing accommodation for international students/medics. This processing is of low risk to the data protection rights of the individuals and does not involve the large-scale use of special category or criminal offence data. It is therefore not necessary for Prima to designate a representative in the European Economic Area (EEA) in order to comply with EU data protection regulations.

Prima (on occasion) processes personal data in connection with rehousing former Asylum seekers with varying confirmed immigration status, either refugee status or leave to remain either indefinitely or for a fixed time period. Prima will also (on occasion) process personal data in connection with rehousing former EU citizens with settled status. This data would not be shared with any third party outside of the UK.

Although unlikely to apply in any circumstance, Prima is aware of the following guidance from the ICO and will implement if necessary:

The EU GDPR adequacy decision does not cover personal data transferred from the EEA for the purposes of UK immigration control, or data which would otherwise fall under the scope of the immigration exemption in DPA 2018. EEA organisations can still make these transfers using an appropriate safeguard from the EU GDPR.

On 2 February 2022, the Secretary of State laid before Parliament the international data transfer agreement (IDTA), the international data transfer addendum to the European Commission's standard contractual clauses for international data transfers (Addendum) and a document setting out transitional provisions. The documents were issued under Section 119A of the Data Protection Act 2018 and following Parliamentary approval came into force on 21 March 2022.

Exporters (of personal data) can use the IDTA or the Addendum as a transfer tool to comply with Article 46 of the UK GDPR when making restricted transfers.

The IDTA and Addendum replaced standard contractual clauses for international transfers. They take into account the binding judgement of the European Court of Justice, in the case commonly referred to as "Schrems II".

These documents are immediately of use to organisations transferring personal data outside of the UK: International data transfer agreement and guidance | ICO

The UK GDPR sets out seven key principles:

- Lawfulness, fairness and transparency.
- Purpose limitation.
- Data minimisation.

- Accuracy.
- Storage limitation.
- Integrity and confidentiality (security).
- Accountability.

The Executive Director of Insight and Group Services has overall accountability for ensuring compliance with all Data Protection legislation and shall ensure that:

- Prima Group is registered as a Data Controller with the ICO.
- Individuals processing personal information understand that they are responsible for complying with the Data Protection principles.
- Individuals processing personal information are appropriately trained to do so.
- Individuals processing personal information are appropriately supervised.
- Individuals are aware of the process to follow if they have any queries when handling personal information.
- Enquiries about handing personal information are dealt with promptly and courteously.

4 Definitions

Data means information which:

(a) Is being processed by means of equipment operating automatically in response to instructions given for that purpose.
(b) Is recorded with the intention that it should be processed by means of such equipment.
(c) Is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system, i.e., highly structured readily accessible paper filing system.
(d) Does not fall within (a), (b) or (c) above but forms part of an accessible record; or
(e) Is recorded information held by a public authority and does not fall within any of paragraphs (a) to (d).

Data Controller means a person who (either alone, jointly or in common with other persons) determines the purposes for, and the manner in which, any personal data is processed. A Data Controller may also act jointly with another organisation to process personal data.

Data Processor, in relation to personal data, means any person (other than an employee of the Data Controller) who processes the data on behalf of the Data Controller.

Data Security Breaches, means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to the shared personal data.

Data Subject means an individual who is the subject of personal data.

Data Subject Rights. Data Subjects have rights in relation to their personal data under the UK GDPR. Those rights include:

(a) The right to be informed.
(b) The right of access.
(c) The right to rectification.
(d) The right to erasure.
(e) The right to restrict processing.
(f) The right to data portability.
(g) The right to object; and
(h) Rights in relation to automated decision making and profiling.

Personal data means information which:

(a) Relates to a living individual who can be identified from the data, or
(b) From the data and other information, which is in the possession of, or
(c) Is likely to come into the possession of, the Data Controller and includes any expression of opinion about the individual and any indication of the intentions of the Data Controller or any other person in respect of the individual.

5 Making sure we do what we say

Prima Housing Group and Prima Commercial are registered with the ICO . The ICO will be notified of any changes in the way in which Prima Group processes personal data within 28 days of the changes taking place.

To show accountability and compliance with the UK GDPR and the DPA 2018, Prima Group keeps all processing activities within its Information Asset Register (IAR). The IAR records the following information against all data assets:

- The source of the data.
- What the data is used for.
- What the data consists of.
- Details of the information asset owner.
- Details of personal and/or special category data contained within the data asset.
- Who has access to the data asset internally.
- Who the data asset is shared with externally.
- Format of the data asset.
- Where the data asset is stored electronically and/or physically.
- Details of the retention period of the data asset and the deletion schedules that are in place.
- Details of the primary processing purpose for the data asset and any other processing purposes.
- Details of the lawful basis identified to process the data asset.

The purpose of the IAR is to:

- Ensure that all personal and special category data is processed under the appropriate legal basis.
- Ensure that all documents are stored in accordance with the agreed retention levels.
- Ensure that all information is only held for the amount of time in accordance with applicable laws and regulations around retention, is not kept longer than is necessary and within statutory guidance.

This policy will be reviewed as and when needed, but annually as a minimum.

Prima Group will commission external auditors to carry out Data Protection Audits to ensure compliance with the UK GDPR and the DPA 2018. In addition, internal audits will be carried out regularly to ensure the importance of following data protection processes is understood by employees and these are followed and embedded.

Data Protection Audits are conducted to:

(a) Raise awareness of Data Protection amongst employees.
(b) To demonstrate Prima Groups commitment to, and recognition of, the importance of Data Protection.
(c) To ensure all Data Protection policies and practices are adhered to.
(d) To identify any potential Data Protection risks we may have been previously unaware of; and
(e) To identify any potential training gaps.

Prima Group will provide mandatory annual training to all employees on the importance of Data Protection and their responsibilities. Training will also be provided to new employees as part of their induction.

Data Protection Impact Assessments (DPIAs) will be carried out for all new activities using personal information prior to work commencing.

Any DPIA that results in a high residual risk, after all possible mitigations, but which can be objectively justified by the Senior Management Team, i.e. the Executive Leadership Team (ELT) and the Executive Management Team (EMT), will be discussed with the ICO for further advice.

If Prima Group hold any overseas data collected before 01 January 2021 (referred to as 'legacy data'), this will be subject to the EU GDPR (known as 'frozen GDPR'). In the short-term, there is unlikely to be any significant change between the frozen GDPR and the UK GDPR. and this is likely to remain the case until 27 June 2025.

Personal data acquired since 01 January 2021 that is processed on the basis of the Withdrawal Agreement is also subject to the frozen GDPR.

Prima will continue to monitor the ICO website for updates, as a result of which:

- Prima may need to be able to identify any personal data collected before the end of 2020 about individuals located outside the UK.
- Prima may need to be able to identify any new non-UK personal data we process because we're complying with the provisions of the Withdrawal Agreement.

6 Other things to consider

6.1 Policies and Procedures

This Policy should be implemented in line with the following related Policies and Procedures:

- Privacy Statement.
- Data Sharing Procedure.
- Data Breach Procedure.
- Subject Access Request Policy, Procedure and Amendment to Tenant Records Procedure.
- ICT Usage Policy.
- Code of Conduct.

6.2 Legislation and Guidance

The UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA) were both amended on 31 December 2020 to make them work as UK law, now that EU law no longer applies in the UK. The two pieces of legislation need to be read together and aren't complete as standalone documents

The correct up-to-date text can be referred to here legislation.gov.uk:

- The UK GDPR
- The DPA
- The Privacy and Electronic Communications Regulations 2003 (PECR)

The UK GDPR is very similar to the EU GDPR, but there are some differences. It contains 99 Articles and 173 Recitals. The articles are legally binding and form the backbone of our data protection legislation. The recitals are separate and advisory only to give context to the articles.

The DPA contains extra UK provisions.

PECR covers electronic marketing including phone calls, emails and texts.

The key principles, rights and obligations remain the same. However, there are implications for the rules on transfers of personal data between the UK and the EEA.

The UK GDPR also applies to controllers and processors based outside the UK if their processing activities relate to:

- Offering goods or services to individuals in the UK; or
- Monitoring the behaviour of individuals taking place in the UK.

There are also implications for UK controllers who have an establishment in the EEA, have customers in the EEA, or monitor individuals in the EEA. The EU GDPR still applies to this processing, but the interaction with European data protection authorities has changed.
The Data Protection and Digital Information Bill is currently working its way through Parliament.

Processing, in relation to information or data, means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data.

Special Category Personal Data, includes, but is not limited to:

(a) Political opinions.
(b) Religious beliefs or other beliefs of a similar nature.
(c) Ethnicity.
(d) Trade union details.
(e) Medical records; or
(f) Sexual preferences.

The ICO governs Data Protection for the UK.

6.3 Privacy and Confidentiality

The Privacy Statement on the Prima Group website details how Prima collects, store, process and retain employee and customer information.

The Privacy Statement will be reviewed on an annual basis to ensure it remains relevant and will be updated with any relevant legislative and/or regulatory changes as and when they occur.

Prima Group regularly reviews its Information Asset Register to ensure it is accurate and relevant.

6.4 Data Sharing

Prima Group will ensure that appropriate safeguards are in place for all information that is shared with other organisations.

Prima has a Data Sharing Procedure which sets out the process to follow when sharing information. The ICT Usage Policy sets out how equipment should be used to further

protect our customer and employee data.

Prima Group will ensure that all data shared outside of the business will be transferred in a secure, safe method and will only share information that is necessary for the purpose.

Prima Group commits to informing all customers and employees on the organisation we share their information with. A full description of the types of organisations we share information with can be found in the Privacy Statement located on our website.

Prima Group will ensure that for all procurement contracts which result in the sharing of personal data, that appropriate safeguards are in place.

6.5 Right of Access Requests

Prima Group will ensure that all customers and employees are aware of their individual rights and how to submit a Right of Access Request, commonly known as a Subject Access Request. This information can be found in the Privacy Statement on our website.

Individual Rights include, but are not limited to:

(a) The right to be informed.
(b) The right of access.
(c) The right to rectification.
(d) The right to erasure.
(e) The right to restrict processing.
(f) The right to data portability.
(g) The right to object.
(h) Rights in relation to automated decision making and profiling.

Prima Group will exercise any relevant exemptions, permitted by the UK GDPR, where necessary, which include:

(a) National security.
(b) Defence.
(c) Public security.
(d) The prevention, investigation, detection or prosecution of criminal offences.
(e) Other important public interests, in particular economic or financial interests, including budgetary and taxation matters, public health and security.
(f) The protection of judicial independence and proceedings.
(g) Breaches of ethics in regulated professions.
(h) Monitoring, inspection or regulatory functions connected to the exercise of official authority regarding security, defense, other important public interests or crime/ethics prevention
(i) The protection of the individual, or the rights and freedoms of others; or
(j) The enforcement of civil law matters.

The Subject Access Request Procedure sets out guidelines on the process to follow when

a customer or employee submits a Right of Access Request.

6.6 Security of Data

Prima Group will ensure that all customer and employee data is held on secure systems and software that restricts access to only those who are required to process the information. When employees are using personal devices for work it is their responsibility to ensure the devices are secure and that no Prima data is stored locally on a personal device as per the ICT Usage Policy.

For any external company that Prima Group may use, we would expect them to adhere to UK GDPR and would ensure appropriate safeguards are in place should they process any data.

6.7 Direct Marketing

Prima Group will use direct marketing to keep all customers updated on, matters linked to their tenancy, community events and provide information relating to each neighbourhood. We use the following methods to provide these types of information to our customers:

- Newsletters.
- Texts.
- Social media.
- Live web chat.
- Customer app.
- E-mail; and
- Phone calls.

All customers are able to opt out of receiving marketing information at any time and further information can be found in our Privacy Statement on the Prima Group website.

6.8 Data Breaches, incident reporting and management

Prima Group will maintain a Data Breach Procedure, which instructs all employees what process to follow in the event of a data breach.

Prima Group will ensure that all breaches or potential breaches/near misses are recorded within the incident log, thoroughly investigate each breach and use any appropriate lessons learned to continuously improve

Prima Group will ensure that any breaches, which may affect an individual's rights and freedoms, will be reported to the ICO and the data subject within 72 hours of becoming aware of the breach.

7 Consultation

This policy has been reviewed with close reference to guidance from the ICO and is largely set in law. The consultation exercise has been limited to what Prima needs to do to be compliant and has had input from employees and EMT in November 2022.

8 Equality Impact Assessment

Prima welcomes feedback on this policy and the way it operates. We are interested to know of any possible or actual adverse impact that this policy may have on any groups in respect of gender or marital status, race, disability, sexual orientation, religion or belief, age or other characteristics.

The policy has been screened to determine equality relevance for the following equality groups: gender or marital status, race, disability, maternity or pregnancy, sex, sexual orientation, religion or belief, age or other characteristics.

9 Document Control Data

Version:	V42023
Review Date:	November 2022
Name of Reviewer:	Julie Hunter, Risk and Assurance Officer
Owner of the policy:	Group Director of Insight and Group Services
Consultation Panel:	Group Services, EMT, ELT
Change Log:	Page 4 – updated ICO advice and link to ICO website on transferring personal data outside UK Page 4 - Group Director amended to Executive Director Page 8 – Reference to Keeling Schedule removed – UK legislation now updated Page 9 – Reference to Data Protection and Digital Information Bill added Page 11 – Section on CCTV removed – already covered in Privacy Statement
Date approved by EMT:	22/03/2023
Date to Customer Voice Board:	N/A
Date approved by Committee:	AAC – 24/05/2023
Date approved by Group Board:	N/A
Date of Equality Impact Assessment:	02/12/2022
Date due for next review:	March 2024