Plus Dane Housing

# Data Protection Policy

# 1 Policy Statement

Plus Dane Housing Ltd will comply will all of the requirements of the General Data Protection Regulation (GDPR), as well as national legislation developed to support the protection of PII.

*PII* is defined as any information from which an individual could be identified (including information, which, if combined, could reveal the individual's identity). It is described in the Regulation as Personally Identifiable Information (PII).

Plus Dane is committed to preventing unauthorised access and misuse of the PII for which the organisation is responsible. To support this commitment, staff and Board members will subscribe to the following principles:

***Need*** – Plus Dane will only hold the minimum amount of PII required to fulfil its contractual, regulatory, and service obligations, and only for as long as is required for those obligations.

***Access*** – Staff and Board members will only be provided access to PII, based on necessity. Managers responsible for each type of PII controlled by Plus Dane will ensure that the unauthorised disclosure of data is protected against and that mitigation plans are in place to respond to any PII breach.

***Simplicity*** – PII will be held and used in an organised and structured manner. Staff and members will not keep duplicate copies of records, nor will they create or hold paper records, unless absolutely necessary.

***Accountability*** – All Plus Dane staff are to be held responsible for the proper use and management of PII.

## 2 Policy Aims

This policy aims to accomplish the following:

- Explain Plus Dane Housing's obligations as both a Data Controller and Data Processor;
- Detail Plus Dane Housing's approach to implementing and maintaining alignment with the GDPR Article 5 Principles;
- Confirm Plus Dane Housing's commitment and approach to supporting the following data subject rights:
    1. The Right to be Informed,
    2. The Right of Access,
    3. The Right to Rectification,
    4. The Right to Erasure,
    5. The Right to Restrict Processing,
    6. The Right to Data Portability,
    7. The Right to Object, and
    8. Rights related to Automated Decision Making including Profiling;
- Detail Data Protection Roles and Responsibilities, including the role of the Data Protection Officer; and
- Establish requirements for training and evaluation of Plus Dane Housing's data protection measures.

## 3 Links to Corporate Plan

The Data Protection Policy impacts on all "Big 4" corporate objectives, as it pertains to all PII processing, collection, and storage activities.

There are clear financial and reputational reasons to be compliant with the GDPR, including the following penalties:

Up to *€10 million or 2% of annual turnover (whichever is greater)* is the penalty for non-compliance in obligations as the Data Controller or Data Processor, including non-compliance as pertains Privacy Impact Assessments (PIAs) and Data Breach notifications.

Up to *€20 million or 4% of annual turnover (whichever is greater)* is the penalty for non-compliance with key GDPR principles for processing, including conditions for consent, data subject rights, and the transfer of PII to 3rd countries.

Additionally, breaching Data Subjects' rights can lead to litigation. Potential legal costs and damages for a large scale breach could be significantly in excess of any potential ICO fines.

While those penalties are significant, there are also substantial benefits to compliance with the GDPR. These benefits include the following:

- Consolidation of PII into consistent formats and the elimination of duplication of data, reducing risks and costs;
- The increased accuracy and understanding of the PII Plus Dane holds;
- The decrease of actual data breaches (not simply reported breaches);

- Faster response times and lower workloads for staff responding to data subject rights requests and data breaches;
- Higher focus on PII, which could enable forward-thinking strategies to better respond to customer needs and trends; and
- Lower staff and customer uncertainty about how the company uses and manages PII, as well as higher staff and customer confidence that Plus Dane will do the right things to protect and support them.

## 4 Our approach

Plus Dane Housing is a Data Controller, meaning that this organisation has decided that certain PII will be processed to meet certain specific requirements and objectives. This will always be done with a clear lawful basis for processing as determined by one of more the criteria detailed in the Regulation as follows:

- Consent of the Data Subject
- Required to fulfil a contract with the Data Subject
- Compliance with a legal obligation
- To safeguard the vital interests of the Data Subject
- Public interest
- For the purpose of legitimate interests pursued by the Data Controller, except where such interests are outweighed by the rights and freedoms of the Data Subject

Plus Dane will also abide by the further ten lawfulness rules for processing Special Data, which includes

Plus Dane will also act as a Data Processor on behalf of partner organisations under an agreed contract. In these circumstances, the Data Controller will direct Plus Dane as the type of data to be processed to fulfil the contract and be specific about data storage and disposal.

In certain circumstances there will be a requirement for Plus Dane to assume the role of Joint Controller with another partner organisation. This will be done under contract with indemnities established where relevant to ensure that roles and responsibilities are clear and indemnities are established to mitigate any presenting risk.

In order to maintain compliance with the GDPR and relevant UK regulations, limit risks to Data Subjects, and protect the business from financial penalties, Plus Dane's data protection objectives are broken into the following six key activities:

1) Establishment of a Data Protection Officer and supporting staff;
2) Protecting and Supporting Data Subject Rights;
3) Limiting Risks to PII;
4) PII Management;

5) Incident Management; and
6) Governance and Assurance (detailed in Section 5).

Further guidance on these activities is provided as appendices.

### 4.1 Data Protection Officer

As Plus Dane processes large amounts of PII, including sensitive, health, and data relating to children, a Data Protection Officer (DPO) post will be maintained. The DPO shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks referred to in Article 39 of the GDPR. The DPO is an existing staff member, however Plus Dane is empowered under the Regulation to revisit this with a view to fulfiling the designated tasks via a service contract.

Plus Dane will publish the contact details of the DPO in both its privacy notices as well as providing them to the ICO. Contact information for the DPO will also be made available to data subjects at the point when their PII is first collected. To support this, a DPO email address and page on the Plus Dane website will be maintained.

### 4.1.1 DPO Responsibilities

The Data Protection Officer is responsible for the following:

- To ensure Plus Dane Data Processor and Data Controller adherence to this Policy and relevant data protection regulations;
- To monitor compliance with this policy and relevant data protection regulations, including the assignment of responsibilities, awarenessraising, and training of staff involved in processing operations, and the related audits;
- To provide advice to Plus Dane staff, partners, and customers, when necessary;
- To provide the People & Governance Committee with regular information regarding the number and materiality of data breaches together with a summary of the improvement actions;
- Maintain accurate and complete records of processing operations relating to the core Data Protection processes;
- To cooperate with the ICO; and
- To act as the contact point for the ICO on issues relating to processing and to consult with the ICO, as needed, with regard to any other relevant matter.

The DPO will, in the performance of his/her tasks, ensure that attention is paid to the risks of processing PII, versus the purpose, justification, scope, and context of that processing. Embedding a Privacy By Design approach to all data processing activity and processes will be a fundamental objective for the DPO.

### 4.1.2 Data Protection Office

The Governance and Assurance Officer will oversee the core data protection policies and the compliance with timelines and deadlines. However, the final authority and accountability for the responsibilities of the DPO rests with the individual appointed to that position.

### 4.1.3 Data Protection Champions

Data Protection Champions from within the core business have been established to provide ongoing assistance towards the implementation of improved data protection throughout the business. These champions are a critical aspect of embedding the cultural shift towards a Privacy By Design approach to data protection. They will also, in accordance with their terms of reference, help the business maintain adherence to data protection regulations and policies. Data Protection Champion duties include:

- Liaise with the Data Protection Office and Data Protection Officers, regarding data protection practices in their service areas;
- Ensure the Data Register for their service area is up-to-date and accurate;
- Participate in training and be the conduit for building capacity in the teams that sit within their service area;
- Provide service area-specific training to their teams;
- Provide advice to their teams, as needed;
- Carry out self-inspections of their teams, as required by the Data Protection Officer; and
- Advise and assist Data Asset Owners in contractual, procedural, technical, and physical data security.

#### 4.1.4 Data Asset Owner

A Data Asset Owner is any designated senior manager who is responsible for the data processing activities of his or her service area or team. The Data Asset owner has the following responsibilities:

- Ensures that the PII, for which he or she is responsible, is managed professionally, responsibly, and securely;
- Overall accountability for maintaining and managing up-to-date Data Sharing Agreements and contracts to ensure that the privacy of data subjects is protected and that third parties are adherent to the GDPR and contract obligations;

- Ensures that delegated staff have the training, procedures, and tools necessary for the protection of processed PII;
- Supports the response to data breaches within his/her service area, the implementation of mitigating actions, and ensures that lessons learned are adopted;
- Supports the response to Subject Access Requests his/her service area and
- Ensures that the PII held and processed is accurate, up-to-date, backed up, and inventoried/registered.

### 4.2 Protecting and Supporting Data Subject Rights

#### 4.2.1 Right to be Informed

The right to be informed requires an organisation be transparent about it will use PII. A Data Subject must be given information about how his/her data will be processed, when the data is initially collected, and any time previously collected data will be used in a processing activity for which consent was not already given. This information is presented as a Privacy Notice, which is

published on the Plus Dane website. It is reviewed regularly, written in clear and plain language so as to be accessible to many.

### 4.2.2 Right to Access

Data Subjects have the right to access the PII that Plus Dane holds. Access enables an individual to be aware of and verify the lawfulness of the processing of his/her PII.

Individuals have the right to obtain:

- Confirmation that their data is being processed;
- Access to their PII; and
- Other supplementary information – this largely corresponds to the information that should be provided in a privacy notice (how and why his/her PII is being used).

Plus Dane has established a clear process for the management of Subject Access Requests that is fully compliant with the Regulation and will ensure that Data Subjects are able to access their PII where it is determined that a legitimate request has been raised.

There are a number of supporting processes all related to Subject Access detailed in the paragraphs that follow. Processes to ensure that these requests can be managed within the deadlines set out within the Regulation have also been developed and are being actively managed to ensure that Data Subjects' access rights are prioritised.

### 4.2.3 Right to Rectification

Data Subjects have the right to have their PII rectified, should it be incorrect or incomplete. This right extends to data which is being processed by third parties.

### 4.2.4 Right to Erasure “The Right to be Forgotten”

The right to erasure is the right of a data subject to have his/her PII deleted or destroyed, where there is no compelling justification for its continued processing.

### 4.2.5 Right to Restrict Processing

Data subjects have the right to block processing of their PII. Once restricted, the PII can be stored, but not processed. When processing is restricted, only the minimum amount of data required for future processing will be stored.

This action could be taken when a data subject is concerned about incorrect or incomplete data being used to make a judgement which impacts him or her (e.g., an application for a service or offer). The processing of that data could be restricted until the “rectification” claim has been fully processed.

### 4.2.6 Right to Portability

The right to data portability allows individuals to obtain and reuse their PII for their own purposes across different services. It allows them to move, copy, or transfer PII easily from one IT environment to another, in a safe and secure way, without hindrance to usability. It enables consumers to take advantage of applications and services, which can use this data to find them a better deal, or help them understand their spending habits.

The right to data portability only applies:

- To PII an individual has provided to Plus Dane;
- Where the processing is based on the individual’s consent, or for the performance of a contract; and
- When processing is carried out by automated means.

It is important to note that this right only relates to automated processing, and any team wishing to implement an automated process must consult with the Data Protection Officer.

### 4.2.7 Right to Object

Data subjects have the right to object to processing of their data in the following circumstances:

- Processing based on legitimate interests (business need) or the performance of a task in the public interest/exercise of official authority (including profiling);
- Direct marketing (including profiling); and
- Processing for purposes of scientific/historical research and statistics.

A data subject, staff member or customer, could object to the processing of his or her PII at the point of first collection, by denying consent, or during the course of that data being processed. However, if processing is justified, or necessary for the fulfilment of a contract, that data subject could be left without service or incapable of fulfilling a contract. Such a situation could result in the inability of Plus Dane to engage in, or maintain, a contractual agreement with that data subject.

### 4.2.8 Rights related to Automated Decision Making (including Profiling)

Automated individual decision-making is making a decision, which impacts an individual, solely by automated means (no review by a person). Profiling is a form of automated decision-making in which PII is analysed to evaluate certain characteristics about a person (e.g., racial profiling, age profiling, or profiling based on socio-economic status).

## 4.3 Limiting Risks to PII

### 4.3.1 Justification for Processing

The most critical method by which Plus Dane will ensure that risks to Data Subjects' PII are minimised will be to only hold as much data as is justifiable and required for processing. There are six lawful bases, upon which processing can be justified.

The lawful bases for processing are set out in Article 6 of the GDPR. At least one of these must apply whenever you process PII:

**(a) Consent:** the individual has given clear consent for the processing of their PII, for a specific purpose.

**(b) Contract:** the processing is necessary for a contract between the organisation and the individual, or because they have asked Plus Dane to take specific steps before entering into a contract.

**(c) Legal obligation:** the processing is necessary in order to comply with the law (not including contractual obligations).

**(d) Vital interests:** the processing is necessary to protect someone's life.

**(e) Public task:** the processing is necessary in order to perform a task in the public interest or for any official functions, and the task or function has a clear basis in law.

**(f) Legitimate interests:** the processing is necessary for the organisation's legitimate interests, or the legitimate interests of a third party, unless there is a good reason to protect the individual's PII which overrides those legitimate interests.

Plus Dane has captured the lawful basis for processing each type and category of data that it holds within the Data Register and this will be maintained on an ongoing basis and updated as new datasets are added.

### 4.3.2 Data Protection Impact Assessment (DPIA)

A Data Protection Impact Assessment (DPIA) is a process by which to identify and mitigate risks to PII. A DPIA must be conducted when a processing activity changes significantly, to include technological changes, and when new or current processing activities are likely to place the rights and freedoms of data subjects at high risk. The following are examples of high-risk processing activities (this list is not exhaustive):

- Systematic and extensive processing activities, including profiling and where decisions that have legal effects, or similarly significant effects, on individuals.
- Large scale processing of special categories of data or PII relation to criminal convictions or offences. This includes processing a considerable amount of PII at regional, national, or supranational level; that affects a large number of individuals; and involves a high risk to rights and freedoms (e.g., based on the sensitivity of the processing activity).
- Large scale, systematic monitoring of public areas (CCTV).

As all major changes to systems and processes will go through some form of formal decision making as part of the Plus Dane governance framework, project and process leads are required to make a mandatory consideration as to

whether the processing of personal data is in scope as part of the change. Where this is confirmed, a formal DPIA will be completed and signed off by the DPO prior to submission for decision.

### 4.3.3 Digitisation of PII

Service areas will maintain PII holdings solely in digital format, unless doing so is overly onerous or complex. If PII exists in electronic format, Plus Dane staff will not hold duplicate paper copies of that data. Access to electronic data will be technically limited (e.g., password protected, encrypted, physically separated), and if doing so is impossible, the issue will be escalated to the DPO.

The service area that owns a particular set of data will coordinate with the IT team to ensure that electronic PII files are backed up and technologically secure.

Information is not permitted to be held on personal digital accounts and hardware. If stored on Plus Dane shared drives, emails, and spreadsheets, those PII holdings will be logged on the Data Register, with staff and partners encouraged to create local inventories.

### 4.3.4 Limiting Access to PII

Access to PII will be limited to those who erquire access in order to fulfil their role. If an individual does not have justification for accessing PII, that person will not attempt to view or utilise that data. Any unlawful access to data may involve the individual being held to account via disciplinary and/or legal means.

To support governance of PII access, service area Data Asset Owners are encouraged to create and maintain Access Rosters, stating the personnel, internal and external, who should have access to type or grouping of PII.

### 4.3.5 Physical Data Management and Restrictions

As detailed in the Information security policy, staff and partners are expected to protect all information holdings. This includes locking computers, securing document and information sharing sites, locking shared folders, and preventing unauthorised access to certain systems.

In terms of document protection, staff will ensure that paper documents are discarded in confidential waste bins or shredders. Teams are also encouraged to support the implementation of a “clean desk” principle for the organisation, the benefits of which being cleanliness, standardisation, and security of physical documents. Confidential waste should be retained until it can be

securely disposed of in the designated waste bins or shredders where people are working away from the office.

### 4.3.6 Data Sharing with Third Parties

A third party is a person or organisation that does not fall under the responsibility of Plus Dane. Examples of third parties include, but are not limited to, external suppliers, consultants, solicitors, contractors, partner organisations, and governing bodies.

Any contracts that Plus Dane enters into that requires the sharing of PII will be accompanied by a Data Sharing Agreement (DSA). Where Plus Dane is in the role of Data Controller this will be instigated by Plus Dane with Data Processors requested to sign and return the agreement before any personal data is shared. The Contract Owner will be responsible for establishing the DSA, supported by the Procurement Team.

The Data Controller will always be the responsible and accountable party, as concerns the PII that the Data Controller is sharing. The Data Processor is only contractually liable, in terms of the documented instructions and expectations of the Data Controller.

DSAs will specify the subject matter, duration of processing, the nature and purpose of processing, the type of PII to be processed, the category of data subject involved, and the obligations and rights of the Controller (further detail is provided in the appended guidance).

Any activity requiring data processing in a non-EU country will be elevated to the DPO for consultation and approval, to confirm any special provisions that will need to be implemented.

## 4.4 PII Management

In order to satisfy the requirements of Article 30 of the GDPR, Plus Dane will identify and monitor the PII for which it is the Data Controller or Processor. Plus Dane will adhere to this Article by maintaining a Data Register and PII Inventory. The Data Protection Officer has responsibility for the Data Register and Data Inventory.

### 4.4.1 PII Register

A Data Register is maintained to document the PII processing activities undertaken by Plus Dane service areas. The following is captured within the Data Register:

- The name and contact details of Plus Dane Housing, and where applicable, the contact details of other Controllers and representatives;

- The name and contact details of the Data Protection Officer (DPO);
- The justification for each processing activity;
- The purposes of each processing activity;
- A description of the categories of individuals and categories of PII used;
- Identification of child and Special Category data processing;
- The categories of recipients of PII;
- Details of all transfers to third countries, including documenting the transfer mechanism safeguards in place;
- The volume of data being processed;
- Data Retention Schedules; and
- A description of applied technical and organisational security measures.

The DPO will ensure that Data Asset Owners review and update the PII Register quarterly, at a minimum. Additionally, Data Asset Owners will ensure that any changes to their data processing and assigned roles are reflected as soon as possible on the Data Register.

### 4.4.2 Data Inventory

In order to have a full account of Plus Dane Housing's PII holdings, and support requests by Data Subjects to exercise their rights, a Data Inventory is maintained. The Data Inventory details all PII held, in reference to a particular individual's unique reference number (e.g., employee reference number or tenancy reference number). This overview data is extracted from the systems on which PII is stored.

The Data Inventory's accuracy relies upon data being correctly managed in Plus Dane's systems. As such, the DPO will ensure that Data Asset Owners are properly managing their PII within their relevant systems.

As the Data Inventory cannot extract summary data from paper records, paper record information or inventories will be supplied to the DPO, ideally via spreadsheet. The DPO will direct the format of those inventories and ensure that they are updated quarterly, at a minimum.

### 4.4.3 Data Retention

The Data Retention Schedule is recorded and managed as part of the Data

Register. The Data Protection Champions, in consultation with Data Asset Owners, are responsible for maintaining data in accordance with the retention schedule.

### 4.5 Responding to Incidents

#### 4.5.1 Data Breach

A data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of a single or multiple Data Subjects' PII. In short, there will be a data breach whenever any PII is lost, destroyed unlawfully, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable and this unavailability has a significant negative effect on individuals.

Data breaches can include:

- Access by an unauthorised third party;
- Deliberate or accidental action (or inaction) by a controller or processor;
- Sending PII to an incorrect recipient;
- Computing devices containing PII being lost or stolen;
- Alteration of PII without permission; and
- Loss of availability of PII that is not due for removal or destruction.

Upon notification of a suspected data breach, the DPO has 72 hours in which to confirm the breach and determine whether the severity is such that the ICO is made aware. The DPO will make a data breach determination and risk assessment within 24 hours of the breach being reported.

The Data Subject impacted by a breach may also need to be notified if it is deemed that they will need to take action to mitigate any personal risk.

Teams should always raise suspected data breaches, as failure to do so could increase the probability of data subjects being negatively impacted by them, and to a greater magnitude. The DPO maintains a register of suspected and actual data breaches, which are reported to People and Governance Committee quarterly as part of the balanced scorecard.

# 5 Assurance

## 5.1 DPO INDEPENDENCE

In order to prevent conflicts of interest, or the appearance thereof, the DPO will report to the Board of Plus Dane. The DPO will also avoid fulfilling other duties if they could result in conflict of interest. If the DPO determines a conflict of interest in a particular situation, the Company Secretary will fulfil the responsibilities of the DPO, in that situation.

The appointed DPO should not be penalised for fulfilment of his/her duties, and as such, any decision to terminate an appointed DPO will require Board approval.

## 5.2 Audit and Training

Compliance with data protection legislation will be assessed via the Internal Audit programme. Plus Dane staff and members will be required to complete initial data protection and annual refresher training. Audits and training, relating to PII protection, will be monitored by the DPO and his/her office.

## 5.3 Reporting

### 5.3.1 Executive Management Team (EMT)

All reporting will be channelled through EMT to maintain situational awareness and enable necessary actions to be considered and proposed to Board.

### 5.3.2 Board

The primary reporting channel will be through People and Governance Committee to Board, where KPIs will be reported at each committee meeting. Additional reporting may be required on an ad-hoc basis for such instances as a high risk data breach.