

## **Legal, Security and Privacy FAQs for customers from United Kingdom and Europe**

Capitalized terms are defined in the PCS MSA or DPA available [here](#).

### **What terms do apply to our purchase of PCS services and HW?**

- When you purchase services from PCS, you enter into an online or offline Order Form governing the purchase that is subject to our Master Services Agreement based on your region and available [here](#).
- There are also limited product specific terms outlined in the Product Addenda also available [here](#).

### **How does PCS ensure compliance with data protection regulations like GDPR and what terms apply to the processing of personal data on our behalf?**

- PCS is committed to GDPR compliance and other data protection regulations through comprehensive data processing agreements and processes that respect your data rights.
- We enter into a comprehensive Data Processing Addendum as part of our Master Services Agreement. Both documents are available [here](#).

### **What privacy and security measures does PCS have in place to protect my data?**

- We use a range of security measures, including encryption, access controls, and secure data storage, to ensure your data is protected. The details are available in our Security and Privacy Documentation available [here](#).

### **Where is my data stored, what infrastructure and subprocessors PCS uses?**

- We use reputable companies for sub-processing such as Microsoft and store the resident data in the UK and/or European Economic Area.
- Specifically, for our mCare Services, we store the resident data in the EEA with Microsoft.
- You can view a detailed list of our infrastructure and subprocessors listed per product in the Infrastructure and Subprocessors documentation available [here](#).

### **Are you storing the resident data outside of the United Kingdom and European Economic Area? What transfer mechanisms do you have in place?**

- No. As explained above, for mCare Services we store the resident data in the European Economic Area. For other services, we can use the storage in the United Kingdom or in the European Economic Area.
- For non-storage purposes there can be further transfers of the personal data in the meaning of the applicable privacy laws.
- As we are a UK business, there is no international transfer established between our customers and ourselves. If there is an onward transfer, we commit to comply with the GDPR requirements, specifically Chapter V with our transfers.
- The information about the location of storage and processing is available in the Infrastructure and Subprocessors documentation available [here](#).

### **What happens if there is a data breach involving my information?**

- In the unlikely event of a data breach, PCS follows a strict protocol for detecting, notifying affected parties, and mitigating the impact, in accordance with legal requirements and our DPA.
- We also notify you about Customer Data Incidents without undue delay as described in our DPA available [here](#).

### **What product features are included in the purchased services?**

- Each product has its own documentation that is available to our customers.
- The list of product features is available under Product Description [here](#).

### **For what purposes do you process personal data submitted to your services?**

In the course of the provision of the services, PCS processes personal data for the purposes of providing the services to our customers under our agreement. In addition, we may use such personal data to derive Anonymous Data for research and benchmarking purposes, analysing and improving the services as well as preparing aggregated reports and statistics. Using Anonymous Data to identify trends, patterns, and areas for improvement, we mainly aim to:

1. Enable research to enhance the identification of risk and quality of life factors among frail and elderly to provide predictive modelling of the likelihood of health-related outcomes functionality for customers, as well as general research for population health management purposes.
2. Provide benchmarking of resident care outcome metrics for our customers at their locations along with the comparison against industry metrics.
3. Enhance performance and optimise user experiences and our services.

We ensure that data used for analysis is properly anonymised. Directly identifiable personal data is removed or altered to protect individuals' privacy. Techniques such as pseudonymisation followed by anonymisation (aggregation, and generalisation) are employed.

Robust security measures are in place to safeguard Anonymous Data. Encryption, access controls, and regular audits protect against breaches.

### **Is there anything that customers shall inform their data subjects about in regard of PCS processing of personal data?**

Customers are responsible for informing their residents (service users) and staff within a home (location) that:

- their personal data are being processed by Person Centred Software as customer data processor; and
- that Person Centred Software may derive anonymous data for research and benchmarking purposes, analysing and improving the services as well as preparing aggregated reports and statistics. For more information, data subjects may refer to Person Centred Software Privacy Policy.

Such information may be included in Customer's Privacy Policy.