

# Customer Data Protection Policy and Privacy Notice



Telent is committed to handling personal data appropriately, securely and in accordance with relevant legal requirements

Telent meets the requirements of all relevant data protection laws, including the UK General Data Protection Regulation and the Data Protection Act 2018

## **Policy**

As a provider of IT and networking solutions to businesses, Telent does not ordinarily carry out processing of personal data on behalf of our customers. However, on occasion we may need to do so as an ancillary element of our service where we are instructed to do so by our customer, for example the configuration of customer environments and management of network permissions.

Where personal data is processed by Telent on behalf of a customer, we shall:

- process the data 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.
- maintain records of processing activities under our responsibility
- not engage another processor without authorisation from the customer
- make reasonable information available to the customer on request, and allow for and contribute to audits, including inspections, conducted by the customer or another auditor mandated by the customer.
- inform the customer if, in our opinion, an instruction infringes data protection law.
- notify the customer without undue delay after becoming aware of a personal data breach.

## **Telent as Data Controller**

Where Telent is the data controller it will take responsibility for and demonstrate that it processes personal data in compliance with the relevant data protection laws.

## **Details of Data Controller**

Telent Technology Services Limited

Point 3, Haywood Road, Warwick CV34 5AH

Email: [dataprotection@telent.com](mailto:dataprotection@telent.com)

## **Information we may collect from you**

We may collect customer's staff contact details (name, email address, work number and job title) directly from the customer. It is in our legitimate interest to process this information for operational purposes and to fulfil our contractual obligations to them. This information may be hosted by Telent or a third party on or behalf.

Telent has produced supporting policies, procedures and training to implement these requirements.

## **Your Rights**

Under data protection laws, you have rights including:

- Your right of access - You have the right to ask us for copies of your personal information.
- Your right to rectification - You have the right to ask us to rectify information you think is inaccurate.
- You also have the right to ask us to complete information you think is incomplete.
- Your right to erasure - You have the right to ask us to erase your personal information in certain circumstances.
- Your right to restriction of processing - You have the right to ask us to restrict the processing of your information in certain circumstances.
- Your right to object to processing - You have the right to object to the processing of your personal data in certain circumstances.
- Your right to data portability - You have the right to ask that we transfer the information you gave us to another organisation, or to you, in certain circumstances.

We can be contacted at [dataprotection@telent.com](mailto:dataprotection@telent.com) if you wish to make a request. If you have any concerns about how we have used your data, please contact us in the first instance. You also have the right to make a complaint to the Information Commissioners Office.

# Customer Data Protection Policy and Privacy Notice



Telent is committed to handling personal data appropriately, securely and in accordance with relevant legal requirements

## **Privacy by Design**

When designing or implementing solutions for our customers, Telent will aim to put in place appropriate technical and organisational measures to implement the data protection principles set out in UK GDPR to effectively safeguard individual rights.

Telent will aim to minimise the use, access, storage or disclosure of personal data wherever possible unless otherwise instructed by the customer.

## **Security**

Telent holds ISO27001:2013 certification, Cyber Essentials Plus certification, and aligns with HMG InfoSec and Cabinet Office frameworks. Relevant operational areas are further accredited to List X and Public Services Network (PSN).

In addition to a Data Protection Team (comprising of Legal and Security), we have a designated Chief Information Officer (CIO), Chief Information Security Officer (CISO), Senior Information Risk Owner (SIRO) and a Security Working Group.

All Telent staff are vetted to at least the Baseline Personnel Security Standard (BPSS). All of our laptops are encrypted and our mobile devices are subject to mobile device management (MDM).

## **Data Storage**

Telent uses UK based servers unless otherwise instructed by our customers, or, where we use third parties to host our databases, this information may be stored within the EU/EEA. In the case of our Irish business, data may be stored in Ireland.

We store information for no longer than necessary and generally do not retain documents/data for longer than 7 years.

The Senior Information Risk Owner, with support from the Senior Management Team, has overall responsibility to ensure that this policy is effectively implemented and delivered throughout the Telent business.

Managers must ensure that activities within their areas of responsibility are conducted in accordance with this policy and supporting documentation.

All staff must adhere to this policy and supporting documentation. This includes permanent staff, contractors and temporary workers.

## **Review**

This policy, and Telent's performance in meeting its requirements, will be regularly monitored and reviewed at least annually.

**John Kimpton**

**Senior Information Risk Owner (SIRO)**

**Next Review, October 2024 – Issue 7**

## **Responsibilities**