External Provider Standard - Personal Data

Document type: Guidelines

Document ID: 251723

Document classification: Public

Approval date: 01/12/2025

Table of contents

1 Introduction

Starion develops and delivers tailored system engineering services and solutions for space, defence and other critical infrastructures across Europe, and can only do so if everyone working at Starion commits to meet the standards outlined in our Starion Code of Conduct. Our Code of Conduct is underpinned by our values:

- **Integrity** – We insist on ethical conduct in all our endeavours;
- **Inspiration** – Fuelled by passion, propelling us towards excellence
- **Care** – We are committed to individual wellbeing and growth
- **Collaboration** – Generating strength from diverse perspectives through teamwork.

We recognise that any business operating today will manage data and we all must take steps to ensure that the management data in our custody is carried out safely. This is captured through the four pillars of our Compliance Programme:

- **Our Structure** – We meet our legal obligations to trade and operate
- **Our Operations** – From people to services…we operate with excellence
- **Our Growth** – We follow our processes, making the right decisions to grow our business
- **Our Reputation** – We act with integrity and always do the right thing.

One of the types of data where this requirement is particularly important is Personal Data, following the implementation of the General Data Protection Regulation (GDPR). GDPR imposes standards and requirements that impact not only the amount or type of personal data we control or process, but how we implement technical and organisational measures to assure its protection insofar as possible.

Our External Provider Standards are not designed to tell you how to structure or run your business; they are designed to highlight those requirements and enable you, as an External Provider to the Starion, to assess, review and apply rules to the personal data you control or process, and the technical and organisational measures you implement, in a way that is both compliant with legal requirements and right for your business.

We thank you for your support of Starion and we appreciate your co-operation in helping us ensure that you, as one of our External Providers, understand and commit to the same standards as we do within Starion.

Gaëtan Desclée

CEO – Starion

2 Understanding the GDPR principles

The GDPR is built upon seven key principles:

1. **Lawfulness, fairness and transparency**: Data must be processed legally, fairly and in a way that is transparent to the individual. Organisations must inform individuals about how their data is used.
2. **Purpose limitation:** Data should be collected for specified, explicit and legitimate purposes, and not used for other incompatible purposes.
3. **Data minimisation**: Only the minimum amount of data necessary for the intended purpose should be collected and processed.
4. **Accuracy**: Personal data must be accurate and kept up to date. Inaccurate data should be corrected or deleted without delay.
5. **Storage limitation**: Data should be kept only for as long as necessary for the purposes for which it was collected.
6. **Integrity and confidentiality (security)**: Data must be processed in a way that ensures appropriate security, including protection against unauthorised access, loss or damage.
7. **Accountability**: Organisations must be able to demonstrate compliance with all GDPR principles. This includes maintaining records, conducting audits and implementing policies.

These principles are designed to support a risk-led approach to processing Personal Data, which differs for each type of processing and the nature of the business we operate.

We ask our External Providers to operate an approach to Personal Data that embodies the above principles within their business, so that they can demonstrate compliance with the above requirements against a risk-led approach.

3 Defining your technical and organisational measures

If you are a business processing Personal Data (which can be on behalf of your customers like Starion, or internally for your employees) you will have to implement appropriate technical and organisational measures to protect the Personal Data you process, in line with Principle 6 above, and keep records of the Personal Data you process, and how you process it, in line with Principle 7 above. These will include system, environmental and human factor controls.

Starion asks its External Providers:

- To apply the same appropriate technical and organisational measures to the Personal Data they process on behalf of Starion as they apply to their own Personal Data as a minimum standard
- To implement any reasonable technical or organisational measure requests made by Starion in respect of Starion Personal Data they process to meet either our own customer requirements, or comply with GDPR
- To not process Personal Data on behalf of Starion other than in accordance with those technical and organisational measures
- To store and process Starion Personal Data only for the purpose defined by our contractual arrangements.

We ask our External Providers to only process Personal Data in accordance with defined and consistently applied technical and organisational measures within their business, and those defined separately in relation specifically to any Starion Personal Data.

4 Controller or Processor – What's your role?

If you decide why and how Personal Data is processed, you are a data controller under GDPR. This means that it is up to you to determine the framework and requirements associated with the processing of Personal Data, whether you process it yourself or outsource the processing to a third party, who will be your processor.

If you process Personal Data on behalf of Starion, you will be either a processor (where Starion is the controller) or a sub-processor (where Starion is processing Personal Data on behalf of a customer who is the controller). In either case, Starion will have a responsibility to provide processing instructions to you, and to identify and specific technical or organisational measures you are required to implement in respect of Starion Personal Data.

Our External Providers must:

- Guarantee that you process Personal Data received from Starion in accordance with appropriate technical and organisational measures
- Conduct or support Starion in conducting any required Data Privacy Impact Assessments in relation to Starion Personal Data
- Follow the instructions received from Starion and implement them
- If technical and organisational measures cannot be implemented, engage with Starion to seek guidance on alternative measures that can be implemented in line with the GDPR principles
- Process Starion Personal Data only as instructed and for the purposes outlined in our contractual arrangements with you.

We ask our External Providers to engage fully and openly with Starion in in operating as a processor for Starion Personal Data, including implementing protective measures and privacy by design requirements communicated by Starion.

5 Managing your own supply chain compliance

Whether you are a controller, a processor or a sub-processor, you will either process Personal Data internally within your organisation or you may outsource the processing of Personal Data to third parties. These third parties will be your processors or sub-processors.

Personal Data is managed on paper, but predominately through IT systems, software and hardware (Systems). Many businesses externalise their Systems and buy them from specialist third parties. Systems can be owned and operated by you as an External Provider, but those Systems likely contain components that are provided by third parties.

If you outsource the processing of Personal Data that you control or process yourself, or you process using third party Systems or third-party components in your own Systems, you have a responsibility to ensure that those third parties comply with GDPR.

Our External Providers must:

- Identify where they outsource the processing of their Personal Data to a third-party provider and seek Starion approval where this includes the processing of Starion Personal Data
- Understand their Systems end-to-end and be clear about any third parties providing all or part of those Systems
- Understand how Starion Personal Data will be processed within the System
- Assess their third parties for GDPR compliance and have corresponding contractual commitments within their own third-party contracts
- Unless specifically agreed with Starion, only allow Starion Personal Data to be processed within the European Union.

We ask our External Providers to understand and map their own supply chain for processing and system purposes, ensure their supply chain is GDPR compliant and following the instructions of Starion in processing Starion Personal Data through their own supply chains.

6 What to do if there is a data breach

Even though businesses impose technical and organisational measures across their organisations, Systems and supply chain, unfortunately data breaches can happen. In conducting regular assessments of your Systems, audits of your supply chain or considering your technical or organisational measures, you may also come across weaknesses or threats that could result in a data breach.

Whenever a data breach occurs, it is critical you notify Starion as soon as possible, and in any event **within 24 hours** of the breach occurring. This is because Starion will be required to notify its customers (where Starion acts as a processor) or potentially notify the appropriate data protection authorities (where Starion operates as a controller). Your notification must identify:

- The Personal Data impacted
- The nature and volume of that Data
- The cause of the breach
- The steps you have taken to mitigate the breach.

Whenever you discover a breach, you must take immediate steps to mitigate the breach. This may mean isolating systems, restricting access or ceasing processing.

Where you discover a potential breach, you should notify Starion of the corrective actions you have taken as soon as possible, and how those impact the processing activities you carry out for Starion.

We ask our External Providers to comply with notification requirements above in respect of Starion Personal Data they process.

7 Audit

Starion will need to engage with you during our contractual relationship to verify that you continue to process Starion Personal Data in accordance with our contractual arrangements and this Standard. There can be many reasons for this requirement: it may be required by Starion's customers; it may be

required by Starion to meet our external permits and accreditations; it may be required by applicable laws; or it may be required from an assurance perspective.

Unless we cannot do so, we will always provide a reasonable pre-notification of any audit activities we undertake, and the terms of reference of that audit.

Audits may show up issues, particularly risks related to the way you process Starion Personal Data. We will discuss these with you after the audit is completed and agree the steps you need to take to protect the Starion Personal Data you process.

Our External Providers must offer open, transparent and complete collaboration, so that audits can be performed as smoothly as possible and any recommendations swiftly agreed and implemented to protect Starion Personal Data.

8 What if you do not comply with this Standard?

We have specifically designed this External Provider Standard so that it can adapt to your business, while enabling Starion to be comfortable about how you process Starion Personal Data. However, data protection is a serious matter, and failure to comply with GDPR can have serious financial and reputational consequences for everyone involved in the processing chain.

If Starion identifies any External Provider has not complied with this External Provider Standard, Starion may require a rectification plan to be implemented, at the External Provider's cost, or terminate our contractual relationships for cause.

Starion commits to be proportionate in its engagement with you around this Standard and any breaches that occur.