Syx Automations
GANTNER Group Member

GDPR white paper

Your privacy matters

Syx Automations Belgium
Rozendaalstraat 53
8900 Ieper
Tel. +32 (0) 57 22 44 00
Fax +32 (0) 57 22 44 01
info@syx.be • www.syx.be

Syx Automations The Netherlands
Duwboot 13
3991 CD Houten
Tel. +31 (0) 33 43 284 16
Fax +31 (0) 33 46 109 33
info@syx.nl • www.syx.nl

Syx Automations UK
8 Northumberland Avenue
WC2N 5BY London
Tel. +44 (0) 17 82499195
Fax +44 (0) 20 36273443
info@syxautomations.co.uk • www.syxautomations.co.uk

Table of contents

Syx Automations BE
Rozendaalstraat 53
8900 Ieper
T. +32 (0)57 22 44 00
F. +32 (0)57 22 44 01
www.syx.be

Syx Automations NL
Duwboot 13
3991 CD Houten
T. +31 (0)33 43 284 16
F. +31 (0)33 46 109 33
www.syx.nl

Syx Automations UK
8 Northumberland Avenue
WC2N 5BY London
T. +44 (0)1782499195
F. +44 (0)2036273443
www.syxautomations.co.uk

Syx Automations
GANTNER Group Member

1 Intro

As Syx Automations acts as a data processor for our customers, we have written this white paper to inform our customers on GDPR, and on how Syx prepares for GDPR readiness. How we deal with privacy is also published in our privacy notice, which you can find on our corporate website: http://www.syxautomations.com/en/about-us/privacy-notice

2 What is GDPR?

At its core, GDPR is a new set of rules designed to give citizens more control over their data. It aims to simplify the regulatory environment for business so both citizens and businesses can fully benefit from the digital economy.

The reforms are designed to reflect the world we're living in now, where each aspect of our lives increasingly revolves around data. From social media companies, to banks, retailers, and governments -- almost every service we use involves the collection and analysis of our personal data. Your name, address, credit card number and more are collected, analysed and, perhaps most importantly, stored by organisations

The European Commission defined the GDPR (General Data Protection Regulation) as a new set of rules governing the privacy and security of personal data. It intends to give European citizens back the control over their personal data. Its impact won't just be felt in Europe though, as it will have wider implications for companies across the world that hold data on the continent.

These new regulations come into effect on May 25th 2018, and will make major changes to all of Europe's privacy laws. It will replace the outdated Data Protection Directive from 1995.

3 What is personal data?

Personal data is any information that relates to an **identified or identifiable living individual**. Different pieces of information, which collected together can lead to the identification of a particular person, also constitute personal data.

Personal data that has been de-identified, encrypted or **pseudonymised** but can be used to re-identify a person remains personal data and falls within the scope of the law.

Personal data that has been rendered **anonymous** in such a way that the individual is not or no longer identifiable, is no longer considered personal data. For data to be truly anonymised, the anonymisation must be irreversible.

Examples of personal data: name, surname, address, email address, identification card number, location data, IP address, cookie, …

4 Who does the GDPR apply to?

Data subject	A natural person whose personal data is processed by a controller or processor
Controller	A controller determines the purposes and means of processing personal data
Processor	A processor is responsible for processing personal data on behalf of a controller

If you are a processor, the GDPR puts you under specific legal obligations; for example, you are required to maintain records of personal data and processing activities. You will have legal liability if you are responsible for a breach.

However, if you are a controller, you are not relieved of your obligations where a processor is involved – the GDPR puts you under further obligations to ensure your contracts with processors comply with the GDPR.

The GDPR applies to processing carried out by organisations operating within the EU. It also applies to organisations outside the EU that offer goods or services to individuals in the EU.

5 What rights do consumers have?

1.	**Consent**	The consumer is informed in "clear and plain" language. Consent to collect can be withdrawn at any time.
2.	**Correction**	The right to make changes to inaccurate data.
3.	**Data portability**	The right to transfer personal data from one electronic processing system to another.
4.	**Erasure**	The right to withdraw consent and ask personal data to be deleted.
5.	**Access**	The right to know what's been collected and how it's been processed.

6 What data obligations do companies have?

1.	**Limit data collection**	Limit what's being collected and protect the data you have.
2.	**Limit processing**	Processing is limited to the purpose for which the data was collected.
3.	**Impact assessments**	Conduct assessments prior to processing when processing sensitive data that may result in risks to consumers.
4.	**Limit who sees data**	Only authorised individuals can access the data.
5.	**Record keeping**	Keep records of processing activities, including the types of data, time limits, and whether it's being exported to third countries.
6.	**Continuous assessment**	Always check that you are protecting the data.

7 Which data does Syx collect?

When you use **our software products as a visitor**, we collect your personal data. Which personal data is collected depends on your specific situation and use of our software. We can collect the following personal information:

- **Contact information** such as name, first name, gender, address, telephone, when provided by you when you register your profile online (through our web or cloud applications) or when you provide this information directly to a venue for CRM/membership/invoicing purposes.
- **Other visitor related information** can be collected for specific leisure use cases:
    - electronic ID, when a visitor is requested to present his/her e-ID to a card reader to register as a customer;
    - family relationships, in case of purchasing memberships;
    - bank account information for direct debit or invoicing;
    - purchase transactions when purchasing tickets, memberships or products through our different points of sale;
    - medical information in case of childcare registrations;
    - course or activity registration history in case of registering for courses, sport activities or other events;
    - visit information, when you scan tickets, memberships for venue entry.
- **Visitor analytics data** using cookies and google analytics/tag manager, retrieving browser type and version, operating system type and version, IP address, web pages viewed, links clicked.

When you use **our software products as an operator**, we can collect the following personal data:

- Contact information such as name, first name, gender, address, telephone, when provided by you when you register your profile online (through our web or cloud applications) or when you provide this information directly to a venue for CRM/membership/invoicing purposes;
- Time & attendance information;
- Access information, time when you visited a certain infrastructure, room;
- Planning & task information;
- Purchase transactions when purchasing tickets, memberships or products at employee discounts through our different points of sale;
- Uniform measurements, in case this is managed by the venue with our software.

Syx Automations BE
Rozendaalstraat 53
8900 Ieper
T. +32 (0)57 22 44 00
F. +32 (0)57 22 44 01
www.syx.be

Syx Automations NL
Duwboot 13
3991 CD Houten
T. +31 (0)33 43 284 16
F. +31 (0)33 46 109 33
www.syx.nl

Syx Automations UK
8 Northumberland Avenue
WC2N 5BY London
T. +44 (0)1782499195
F. +44 (0)2036273443
www.syxautomations.co.uk

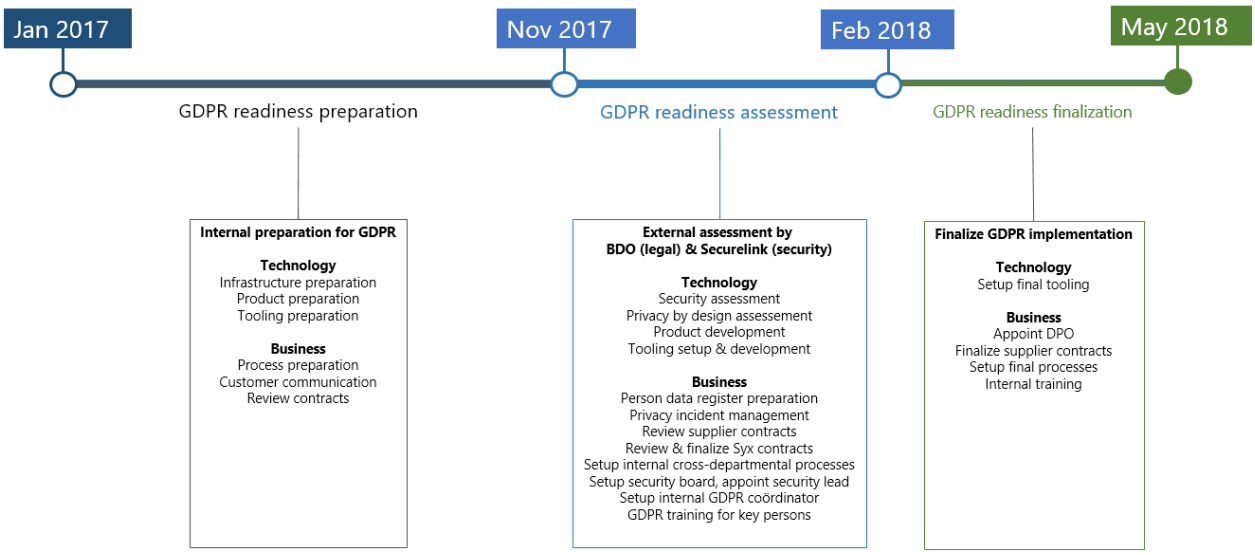
Syx Automations
GANTNER Group Member

8 How does Syx prepare for GDPR?

Syx Automations has started preparing for GDPR since 2017. Our plan exists of 3 phases.

1. **GDPR readiness preparation** – In this phase, we learned what is needed to comply with GDPR as a business, and defined our vision how to comply. From that vision, we outlined key gaps in infrastructure, products, organisation, contracts and process.
2. **GDPR readiness assessment** – In this phase, we requested external legal & security consultants to assess our technology and business, identified remaining gaps and were advised on how to organise ourselves properly for GDPR. BDO supported us mainly on the business and legal needs, performing a thorough review of our existing contracts. We have also set up our data register, and implemented a data breach notification procedure that aligns with our existing incident management procedures.

   SecureLink consulted us on technical security measures, performing a general security assessment of our organisation and a privacy-by-design assessment for our products.
3. **GDPR readiness finalisation –** In this phase, we intend to appoint our DPO, finalise supplier contracts to be GDPR compliant (as we are depending on suppliers' speed of GDPR implementation).



9 What is the status of our GDPR implementation?

Below you find the latest status on **1February 2018**.

9.1 BUSINESS

9.1.1 Organisation

Done

- Defined a vision for GDPR implementation in Syx
- Set up an internal coordinator for the GDPR implementation plan
- Set up a cross-functional senior team to evaluate and implement GDPR (management, HR, sales, development, IT, service, consultancy)
- Set up a security board and an internal security lead, also in line with ISO27001 and cyber essentials
- Adapted job descriptions with security related tasks and responsibilities
- Key people have followed GDPR info and training sessions.

In progress

- We plan to appoint a DPO in the last implementation phase.
- Internal GDPR awareness training

9.1.2 Legal

Done

- Reviewed and renewed our data processing agreement
- Upgrading customers that signed our previous data processing agreement, renewed with latest
- Reviewed our RCX API license agreement for GDPR compliance, including limiting data integration use cases and restricting integration to API, OLAP, controlled database views
- Set up an enviso reselling agreement for GDPR compliance
- Reviewed existing supplier contracts for GDPR compliance
- Signed a data processing addendum with Amazon AWS, for our enviso cloud product

In progress

- Finalise supplier contracts in progress with GDPR implementation
- Review and update the enviso reselling agreement
- Create contractual agreements between Syx Automations NV and our Indian departments for data transfers outside the EU
- Align customers with existing integrations with a new API license agreement

9.1.3 Process

Done

- Set up a GDPR data register
- Privacy impact assessment done for sensitive data
- Set up internal procedures for customer data

In progress

- Setting up a data breach notification procedure, based on our incident management procedure
- Define a data breach risk analysis, to automate risk assessment
- Refining the data retention period for prospect and customer contact data
- Set up a patch management process, based on new tool selection

9.2 TECHNOLOGY

9.2.1 Products & solutions (recreatex)

Done

- Secured all recreatex configuration files
- Enhanced API integration security with a security token on top of password security levels
- Code obfuscation for sensitive code
- Anonymise person data - script

In progress (6.4.1, release end March 2018)

- Support specific consent rules for Scotland
- Adhere to cookie regulation
- Age restrictions in webshop - account level
- Remove sensitive data - employee measurement data
- Implement separate logins per employee for childcare
- Privacy notice integrated by default in webshop
- External privacy assessment

9.2.2 Products & solutions (enviso)

Done

- Implemented privacy-by-design principles
- Publish privacy policy on our landing page
- Publish cookie policy on our landing page

In progress (mass roll-out, end March 2018)

- Report on personal data usage
- Remove / anonymise personal data at request (and in batch)
- Remove / anonymise personal data automated
- Show popup about cookies
- Implementing OWASP security principles

9.2.3 IT infrastructure

Done

- Set up new datacentre in co-location, with Equinix in Amsterdam
- ISO27001 certification
- Two-factor authentication support for new datacentre

In progress

- Cyber essentials certification (for UK market)
- Patch management software selection to automate patch updates

9.2.4 Internal tools

Done

- Script for personal / contact data removal (archiving) in ERP and CRM system
- Script for personal / contact data anonymisation in ERP and CRM system