Sympa

FEEL THE PULSE OF YOUR BUSINESS

SERVICE DESCRIPTION

Sympa HR System

2018

Contents

1 Sympa HR system 3

1.1 Customisable and comprehensive 3

2 Sympa HR as your HR solution 4

3 System features 4

3.1 Multilingualism 4

3.2 User management and user rights 4

3.3 Authentication 5

3.4 Integration to other systems 5

4 Support service 6

5 Data Privacy and GDPR 7

5.1 Sympa HR & GDPR Roles 7

5.2 Sympa HR supports Data Subjects rights 7

5.3 Technical and organisational protection 10

5.4 Processing of Personal Data 13

6 Information security management 14

6.1 Information security controls 15

7 Technology 17

7.1 Client-side requirements 17

8 Software Development 17

8.1 Updates, maintenance, and release cycle 18

1 Sympa HR system

The browser-based Sympa HR system is a global, human-resources information system, combining the processes of human-resources management (HRM), human-resources development (HRD) and recruitment in one consistent entity. The easy-to-use system covers the entire employment life cycle in real time. HR information is up to date at all times and accessible to the appropriate people, and various reporting options are available.

The Sympa HR system is easy to customise to the needs of your organisation. The advanced technology and predefined HR processes enable fast and cost-effective implementation and system extensions and other further modifications, where necessary. Top-class user-friendliness ensures that the human resource processes are smooth and convenient, while the user interface, finalised with the customer's individual graphic layout, ensures a successful user experience on all organisational levels.

This service description document provides an outline and description of the Sympa HR system's HR processes & data contents, most important system properties, support services, information security & continuity and technology choices.

1.1 Customisable and comprehensive

One of the key features of the Sympa HR system is that it can be freely customised. Sympa HR is based on predefined processes, which can be adapted to the customer's own processes and practices at the implementation stage or later on. Customisation can be performed by either the supplier or the customer's trained admin user. Minor modifications should not take more than a few minutes. Entirely new processes and data contents can also be modelled for Sympa HR in accordance with the customer's needs.

The Sympa HR system can cover all HR processes and information related to personnel. The scope of Sympa HR can be decided by the customer, and the system can be expanded at a later stage. Sympa HR has not been needlessly divided into modules; instead, the data contents form a natural whole.

2 Sympa HR as your HR solution

Sympa HR covers the entire employee lifecycle from recruitment to exit interview and provides real-time reports for HR analytics. The processes and methods can be modified easily and adapted to the organisation's needs flexibly.

At the Sympa Best Practice site we've described best practice for the most popular processes as well as for many optional customer solutions and for system features in general.

Log into the site at https://best.sympa.com/ where you can browse best practice in English, Finnish, Swedish and Dutch. Your Sympa contact person will provide you with a password.

3 System features

In this chapter, a number of Sympa HR's key features are described. The Sympa Best Practice site also covers several important features and how they benefit your organisation.

3.1 Multilingualism

The Sympa HR system is multilingual, and the system can be implemented in any language, as required. At the moment, the language options in the system are Finnish, English, Swedish, Norwegian, Danish, Dutch, German, Polish, Spanish, Italian, Estonian, Russian, Chinese, Lithuanian and French. Multiple languages can be used in the same system environment so that, for example, reports can be made in a preferred language in the system irrespective of the language in which the data were entered.

3.2 User management and user rights

The extensive user management feature allows for the modification of user rights and the addition of usernames by the organisation's admin user. If required, the system's user rights can be specified by the Sympa HR supplier.

The users and user rights of the Sympa HR system can be specified freely. Three main user rights groups are used in the Sympa HR system: basic users, manager users and HR users. The user rights include editing rights and reading rights. Where necessary, various special rights can be assigned to individual users or groups, such as management or IT Department.

Admin users with unlimited access to the entire data contents can also be trained for the client. Admin users are also authorised to modify the existing data contents, create new data contents and manage user rights.

Basic user

Basic users have viewing and editing rights over their own details. This means that they can update their address details, sign up for a course or browse job requirements. The basic user can also fill in any competence surveys and prepare for performance reviews by entering details in advance or, if desired, by recording the issues agreed during the review in the system themselves.

The basic users can also compile reports about themselves on the development of their skills or to compare their skills with the targets of their role and with their personal development plan, for example. The basic user's interface has been designed to be as simple as possible so that extensive user training is not required.

Manager user

The manager user has viewing or editing rights over the details of specified persons or a defined group, such as the manager's own team, department or unit. The manager user can use reporting within these content restrictions and compile extensive reports within their area of responsibility.

The required reports for managers can include their team's absences and holidays, a comparison report between two teams, agreed training measures for a group as a summary, or a salary-data comparison.

Admin user

The system admin user has editing rights over the whole system and the data attached to it. Thus, the admin user can modify the contents of the system, and the system will adapt flexibly to the changing requirements. A person in a client organisation receives admin user rights after completing the admin user training organised by Sympa.

The admin user creates the questionnaires, forms and competence profiles that will be used in the system. The user rights and availability times of forms, profiles and questionnaires can be specified on the basis of work duties, for example.

The system admin user can be in the client organisation, at Sympa or both. Through the shared management of admin-user functions we ensure the optimal use of the system, even in case of personnel changes.

3.3 Authentication

There are two ways to set up authentication in Sympa HR: manual login (with a username and password) and Single Sign-On. Both authentications can be used at the same time.

When the Single Sign-On (SSO) method is used, the user login in the Sympa HR system is managed automatically, so that there is no need to enter a separate username and password. In Single Sign-On, the login details are received, for example, from the user's Active Directory login.

The Single Sign-On is based on the SAML 2.0 (Security Assertion Markup Language) standard. The use of SSO requires an authentication server (IdP server) complying with the SAML 2.0 standard. Supported products are Microsoft AD FS 2.0 or higher, Azure AD, and Google G Suite. For other products, please consult your Sympa contact person. Single Sign-on is described in more detail in its own document.

3.4 Integration to other systems

Up-to-date human resources information is necessary for both the organisation's payroll system and many other data systems. Thanks to the agile and extensive interfacial architecture of the Sympa HR system, information related to HR processes can be used in the organisation's other applications as well.

Integrations are remarkably easy and quick to implement in Sympa HR. Integrations enable, for example, to transfer personnel and payroll data between different systems as desired. In this case, the information needs to only be updated in one system, and it is transferred to other applications or from other applications to the Sympa HR system. The most commonly used integratable systems are the payroll system, the working hours system, the user rights application and the enterprise resource planning system (ERP).

The logical interface can also be used for reporting information to third parties so that, for example, payroll clerks can download a range Sympa reports as required. Alternatively, the Sympa HR system can produce a scheduled Excel report for the payroll server. In the same way, by using the interface, it is possible to update or import data efficiently from other systems to the Sympa HR system.

Sympa HR Integration Application programming interface (API) provides a method for exposing data from the Sympa HR solution for integration purposes. An administrator can dynamically create interfaces that provide access, essentially, to any data stored in the HR system. There are no preset/fixed field lists for the interfaces, which means that each interface is, in essence, unique. This gives admin users the option to restrict the transferrable fields only to those required by the calling system, and no unnecessary data is exposed.

As their name suggests, mapping tables are used to specify correlations between Sympa HR and the target system. Thanks to mapping tables, integrations do not require changes in cases, for example, in which new organisational units, such as cost centres, are added to the organisation. The mapping tables are available to admin users.

Data can also be imported to the system as batch imports using Excel. In this way, the history data of other systems can be transferred, during implementation, to Sympa HR for reporting purposes, for example. Batch importing can also be used for the quick updating of salary index increases. Batch imports are carried out by the Sympa HR supplier.

4 Support service

After the Sympa HR system implementation project, our customers' trained admin users are offered support in the system use by Sympa. Our support service offers a central point of contact for dealing with any and all questions and problems related to the Sympa HR system. The support service is available for Sympa HR solutions in production use as well as interfaces between the Sympa HR system and other systems.

The support service provides help in the following:

- Advice on how to use the user interface operations of the Sympa HR system
- Advice to admin users
- Recording tickets
- Communicating the solution to the customer
- Changing the admin user password
- Determining the cause of an error in the Sympa HR system or integration and fixing the problem

The support service does not include the following tasks, which are offered as specialist services:

- Designing the contents of the system
- Modifying the contents of the system
- Amendments to integrations
- Consultation on customer's HR processes
- Batch transfer of data to the system

The support service is available by phone and email on weekdays in English and Finnish between 8 a.m. and 6 p.m. and, in Swedish, between 10 a.m. and 4 p.m. Finnish time, national holidays excluded. The telephone number of the support service is +358 2 9000 1200 and email tukipalvelu@sympa.fi.

The response time of the support service is two working days. The response time refers to the timeframe required for taking a task into processing at Sympa's support services, calculated from the moment of receipt of the ticket. The response time to critical tickets is 30 minutes. All work carried out by the support service, as well as any customer feedback, are reported to the services unit of Sympa and discussed weekly.

In addition to the support service, customers can use the Sympa HR support portal free of charge. The support portal is for Sympa HR customers and distribution partners to ensure transparency of the service. In practice, it is a browser-based, self-service portal where a customer or partner organization can keep track of the progress of personal, or the service requests of the entire organisation and easily send new service requests. By using the support portal, customers and partners can read and follow all system and other releases. There are also Sympa HR tips, guides and other useful material.

5 Data Privacy and GDPR

The provision of the service is based on absolute trust between Sympa and its customers, partners and subcontractors. Sympa inevitably obtains confidential information in customer relationships. Sympa is committed to processing this information carefully and confidentially and to maintaining an information security policy that guides its operations.

5.1 Sympa HR & GDPR Roles

Data Controller

You, as a Sympa Customer, are a data controller. The data controller makes all the decisions about the content, processes and access to data.

Data Processor

Sympa, as a service provider, is a data processor. We process our customers' data only for the purpose of providing the Sympa HR Service. Sympa is responsible to you and also directly to the authorities.

Data Subject

Your employees are data subjects. Typically, these also include freelancers, job applicants, subcontractors, former employees and anyone else, whose data is stored and processed in Sympa HR.

Data Protection Officer (DPO)

Organizations that engage in large scale data processing are required to have a data protection officer.

5.2 Sympa HR supports Data Subjects rights

Privacy by Design

Data privacy and security are the foundation of the Sympa HR service. Our business is processing HR data. We have recognised privacy as a vital necessity for serving our clients.

Privacy is paramount in all our operations including service development, hosting, support services, implementations and also in sales and marketing. Privacy is similarly a priority in current operations and in development projects. We have built and certified our ISMS (Information Security Management System) to ISO27001 standards to demonstrate our compliance and continuous development. Our ISMS and certification covers all our operations and locations.

We continuously evaluate and develop our technical and organisational protection methods as well as risk evaluation processes for better data protection and data privacy. Privacy of your data is our key priority.

Right to be informed

All individuals have the right to be informed about when their personal data is being stored and what data is stored.

Sympa HR:

- Provides legible, easy-to-understand GDPR-proofed templates to use as data privacy documents
- An up-to-date Service Description with details about data use is always available
- In the event that any changes in the service take place that might affect your GDPR compliance, we will let you know

Right to access & Right to rectification

Individuals have the right to access their own data and right to have any incorrect data rectified.

Sympa HR:

- We are a full self-service solution. As the Data Controller, you as our customer can easily choose to make all personal data available for individuals in either ‘read-only’ or ‘read & write’ mode.
- Our customers can also manage the rights, and only the appropriate people will have the right to see the any given piece of information
- Any access to a user’s own personal data is customised according to our customers’ processes
- Self-service applies also for IT integrations: you can manage which data is integrated to and from Sympa HR when integrated with other IT systems
- Sympa HR tools support right to access even in cases where an individual is not able to access Sympa HR directly.

Right to erasure ('right to be forgotten')

Individuals have the right to have their data erased when processing is no longer necessary.

Sympa HR:

- Removing unnecessary data is a standard feature in Sympa HR and can also be automated when it supports your processes.
- Data removals can also be done in several stages. Some data must be stored for longer period of time than other data (for example employment agreements vs. competencies, one-to-one discussions).
- Sympa HR data removal is always secure and disaster recovery systems support GDPR requirements.

Right to data portability

Individuals have the right to have their data provided to them in an easily readable format and also have the right to transmit that data to another controller.

Sympa HR:

- All data that is stored can be exported via the Sympa HR user interface or API.
- Sympa HR offers a quick and easy way to comply with the data portability requirement (due for release to production before May 2018).

Breach notification

Data breaches must be reported to the authorities within 72 hours.

Sympa HR:

- Sympa HR is being monitored and protected 24/7 by separate team of security experts.
- In the unlikely event of breach, we will immediately notify you and provide our customers with instructions on how to notify the authorities and data subjects

5.3 Technical and organisational protection

Sympa's ISMS is built to protect your data. Advanced ISMS and 3rd party information security audits and certifications are the key methods of protection. In addition, we have identified the following technical security features and operating models as key tools in information security and GDPR compliance:

5.3.1 Risk assessments and risk management

Risk-aware thinking is a fundamental part of Sympa's quality management (ISO9001 certified) and information security management (ISO27001 certified) systems. Risk assessment processes include identifying likelihoods, impacts and mitigation and also possibilities related to identified risks. The Protection of Customers' data has been identified as the most critical asset of Sympa. Risk assessment and management processes are audited annually by a third party.

5.3.2 Encryption

All the data *stored in,* and *transferred to/from,* Sympa HR is encrypted with strong encryption algorithms, at rest and in motion.

5.3.3 User management, permissions and authentication

Sympa HR is an HR system where all employees are users by default. Naturally, in some cases, access to the system is limited by the user organisation. Sympa HR is the master system for HR data and typically this data is used by the client in connected IT systems and user management.

Users' access to data can be limited in the system on a need-to-know basis to include only specified persons and limited data set. Typically, most of the data is accessed based on organisation hierarchy, but Sympa HR also supports tailored access rights, for example, for IT users.

Sympa recommends using Single Sign-On (SSO) login and authentication for best user experience and maximum security. SSO login can be used together with multifactor authentication. Sympa HR supports 'username+password' login with password complexity requirements, where SSO is not available.

5.3.4 Logging

Logins and logouts, including failed login attempts, are logged in detail. On the data level, all data approvals are logged and Sympa HR supports storing historical and future data. All changes to data can be logged including details about who changed what and when. The Sympa HR system maintenance team has access to more detailed user action logs and events, in case such data is needed.

Maintenance operations and events in the hosting environment are logged and logs are protected from tampering.

5.3.5 Backups and disaster recovery

Sympa HR is designed and built as a high availability (HA) service where all components are redundant.

Backups from the Customer data are taken daily (changes) with real-time transaction logging. Full back up is taken once per week. RPO (recovery point objective) for disaster recovery is one day. When data loss is caused by human or software error, RPO is 2 minutes.

RTO (recovery time objective) varies based on different disaster levels and is based on risk evaluation process. Loss of primary and redundant hardware has RTO of 60 minutes. RTO for full data centre loss is 7 days.

Daily backups are retained for four (4) weeks. Monthly backups are retained for 12 months except, for attachments, open positions in recruitment, and surveys where the backups are available only for three (3) months. Because backups could contain deleted or erroneous personal data, we offer the possibility to change how long backups are retained. However, we retain backups at least for three (3) months but no longer than 12 months.

5.3.6 Service provider's access to data

Only specified team members in Sympa HR service delivery, maintenance, security and service teams have access to data stored in the Sympa HR service. Access is based on personal credentials and user actions can be tracked on a detailed level if needed. Segregation of duties is implemented based on personal job descriptions. Separate security clearance takes place prior to nomination to most critical roles. The access rights are reviewed or removed regularly and when a person's job or responsibilities change or they leave the company.

5.3.7 Removing data

Personal data can be removed from the system by the Customer. The data removed will stay on disaster recovery systems for a period and will be removed automatically according to backup rotation cycles. Data removals are secure and no data can be restored after it has been removed from backups.

By request, and at the end of the customer relationship, all data is securely removed from the Sympa HR system and databases, including backup systems. Full data removal is coordinated with the customer in such way, that all data can be returned to the customer or transferred to another system prior to erasure.

5.3.8 Hosting, data locations and subcontractors

Our EU customers' data is stored fully within EU datacentres. The primary hosting environment is located in London, UK. Some parts of the service, including offsite backups, disaster recovery, integrations, and features such as binary storages, are delivered from secondary datacentres in the EU. Currently these locations include Germany, Ireland and the Netherlands. We are committed to keeping your data within the EU's borders even after Brexit.

24/7 security services are delivered via the follow-the-sun model. This enables us to have best security experts working full time with full-service availability and security topics. Teams are stationed across the world and come on-shift consecutively ensuring that responses to security incidents and threats come within seconds instead of hours. During the hours of darkness in Europe, security services and service monitoring is delivered from US under the US-EU Privacy Shield agreement.

Hosting providers at the moment include Rackspace (main provider), Microsoft (Azure infrastructure) and Amazon (disaster recovery and optional integration technologies). The complete list of physical data locations and subcontractors is set out in table below.

Sympa HR support services are delivered from Sympa's EU/EEA locations.

Function	Hosting provider	Physical location	Security and Privacy descriptions
Primary hosting location	Rackspace Ltd.	UK, London (LON5)	https://www.rackspace.com/en-gb/information/legal/privacycenter/customer-data-security-and-privacy https://www.rackspace.com/en-gb/security/global-enterprise
Secondary hosting location	Microsoft Azure	Netherlands (Azure West Europe)	https://www.microsoft.com/en-us/trustcenter/cloudservices/azure
Secondary hosting location	Microsoft Azure	Ireland (Azure North Europe)	https://www.microsoft.com/en-us/trustcenter/cloudservices/azure
Disaster recovery	Amazon AWS	Ireland (eu-west-1)	https://aws.amazon.com/security/
Integrations (optional)	MuleSoft Inc. (Amazon AWS)	Ireland (eu-west-1) Frankfurt (eu-central-1)	https://www.mulesoft.com/lp/whitepaper/saas/cloud-security https://aws.amazon.com/security/

5.3.9 Integrations

Data is always transferred using secure SFTP or HTTPS protocols. Integrations can be customised to include only the information necessary. If another system (for example, your payroll system) that has been integrated into Sympa HR only requires an individual's mailing address and not their social security number or any other data, Sympa HR can be customised to share only the address.

5.3.10 Record keeping

As the Data Controller, you will decide beforehand who has access to what information within Sympa HR. By customising user rights (per job role, for example) you can ensure that only the relevant people have access to sensitive data.

As the Data Processor, Sympa maintains a record of all categories of processing activities.

5.3.11 Data minimisation

Data minimisation is very much in keeping with the spirit of GDPR. Sympa HR makes it easy to customise data fields, delete (or correct) unnecessary data and keep your database lean.

We will continue to make usability improvements to the system in order to help you remain compliant, but with less effort.

5.3.12 Data pseudonymisation and anonymization

Sympa HR service monitoring, development and maintenance requires following user actions, system usability and HR processes. Pseudonymisation and anonymization both play an important role in Sympa HR's service delivery. Pseudonymisation and

anonymization enable us to deliver the best possible HR system without using your HR data or any personally identifiable information (PII).

5.3.13 Data Breaches

Sympa HR's security and customer data is monitored and protected 24/7. Sympa has a clearly-defined protocol for identifying, mitigating and informing customers about any possible data breaches.

5.4 Processing of Personal Data

Sympa as the Data Processor offers and maintains an electronic HR system for the customer (Data Controller), enabling the Customer to manage personal data including employment, salary, competencies and other personal data for employees, former employees, job applicants, freelancers, subcontractors and such interest groups as the customer chooses.

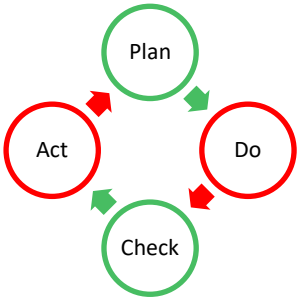
The customer collects, records, analyses and otherwise uses information stored in the HR system on its own account. Sympa does not take part in these activities except by providing a tool that enables the customer to perform these measures and when specifically asked so by the Customer.

Sympa reviews the information stored on the HR system only to the extent necessary to maintain the system for the Customer (including, for example, correcting errors in the system and handling other technical problems in the system). Sympa does not look at the data stored in the HR system more than is necessary to maintain the HR system and related services.

Categories of processing activities are dependent on the Customer's configuration. Categories include gathering data from end users and via APIs, storing data in the service and backup systems, distributing data to end users (reporting) and via APIs, organising and changing data according to the Customer's instructions.

6 Information security management

The Sympa information security organisation is led by Sympa Information Security Manager and DPO Tommi Surakka. Our security organisation takes care of the information security management system (ISMS) of Sympa, including continuous development, risk assessments, information security audits, training and 24/7 monitoring and incident management. Our most critical asset is the data of our customers and we are fully aware of that fact.



Below is an overview of the security organization and security groups. (ISMS controls A6)

Continuous development in P-D-C-A cycles has been the key driver for Sympa HR information security management. Sympa was first granted ISO27001 certification for excellence in information security in 2014 and Sympa has been continually certified since then. The certificate was conferred by Bureau Veritas. Certification covers all operations and locations. The certificate and statement of applicability are available on request.

Sympa HR information security roles and teams in light red boxes. **Information security audits** in light green boxes.

Information Security Manager
- Responsible for Sympa's ISMS

Data Protection Officer
- Monitoring data protection and privacy

Information Security Management Group
- Continuous ISMS development
- Change management
- Regular meetings
- Incident management

Technical Information Security Group
- Technical information security
- Technical security architechture
- Technical security reviews
- Information security code reviews

24/7 Information Security Team
- Monitoring information security and protecting data 24/7
- Rapid response to threats 24/7
- Availability monitoring and repairs 24/7
- Vulnerability scanning
- Security patches,platform and infrastructure management

System Operators
- Proactive security and availability management
- Release management
- Technical information security planning and management in production environment

Internal ISMS audits
- Annual detailed information security audits
- Follow multi-year plan for continuous development
- Audit duration 5–10 days per year

External information security audits
- ISMS is audited against ISO27001 and ISO9001 standards
- Certification since 2014
- Audit duration 3–7 days per year

Technical information security audits
- 3rd party audits for technical information security
- Audits are performed before any major change in Sympa HR Service
- Audits are performed minimum once per year
- Audit duration 5+ days per year

6.1 Information security controls

Sympa's ISMS covers all its operations and locations. Sympa's Information Security Policy (ISMS controls A5.1) is reviewed regularly and is available for review on request. An overview of Sympa's Information Security Management System and the most relevant controls is provided below. A more extensive list of controls is available on request (statement of applicability). Controls have been chosen to meet ISO27001 standards.

6.1.1 Human Resources (ISMS controls A7)

Prior to employment all employees go through an interview and screening processes. Depending on the role, and when roles are changed, a more detailed screening process may take place. Police security clearances are carried out where applicable. All employees sign a non-disclosure agreement before joining Sympa.

During employment, security and privacy awareness is supported by our training programs. At the end of employment, the exit process at Sympa includes access terminations, asset management, change management and interviews to support continuous development.

6.1.2 Asset management (ISMS controls A8)

Asset management includes processes and tools for asset inventory, ownership, data classification as well as guidelines and policies for acceptable use, physical media handling and disposals. The nature of our work means that travelling and working from remote locations is common practice. Our asset protection is based primarily on encryption and protection methods that are location-independent.

6.1.3 Access control (ISMS controls A9)

Sympa's user management and access rights rely on up-to-date HR and subcontractor data managed with Sympa HR. All access and user management processes include named responsibilities and regular reviews. Access to most critical systems is very limited, on a need-to-know basis and protected accordingly, taking into account best practice in multi-factor authentication, restrictions and logging.

6.1.4 Cryptography (ISMS controls A10)

Cryptography is recognized as one of the most important protection methods in technical information security. All critical data is always encrypted in motion and at rest. Special attention is paid to transactions and communication with Sympa HR client organisations and unsecure tools, such as email, are deprecated.

6.1.5 Physical security (ISMS controls A11)

Sympa HR service and critical data is stored in the most secure physical environments. To offer the best possible physical security Sympa has chosen the best hosting providers available. Current hosting environment certifications include ISO27001, PCI-DSS and SSAE16 Type II SOC1, SOC2, SOC3. Access is restricted by biometric authentication, keycards, and 24x7x365 surveillance. Hosting locations are staffed with 24/7 onsite security teams.

6.1.6 Operations security (ISMS controls A12)

Operational safety is based on documented procedures, responsibilities and change and capacity management. Development, testing and production environments are isolated and customers' data is not used in development or testing environments.

Operational environments are protected against malware, information is backed up, operational events are logged and logs are protected against tampering. Installation of software on operational environments is limited and controlled accordingly.

Sympa's operations and information systems are audited regularly. Vulnerabilities are managed and audited in relation to change management and at least once a year to ensure protection against advanced and evolved vulnerability exploits.

6.1.7 Communications security (ISMS controls A13)

All confidential electronic information transfers are encrypted with strong encryption when not transferred within high security isolated networks. All confidential transfers in public internet are encrypted. Networks are always isolated where feasible. Human communications are protected with confidentiality and non-disclosure agreements.

6.1.8 Development & Maintenance (ISMS controls A14)

Development and maintenance processes are monitored carefully by our security team. Product architecture, design and development efforts are evaluated by a separate technical security team. All changes in software are always reviewed before approval for release. All changes in software, including third party component changes, are logged and can be tracked in detail. Quality assurance / testing processes also include security testing and vulnerability scanning and management.

6.1.9 Supplier relations (ISMS controls A15)

Sympa takes full responsibility for its suppliers and subcontractors. Risks related to supplier relations are mitigated with security policies, security practices and guides, supplier agreements including confidentiality and non-disclosure statements. Residual risks are mitigated with information security insurances.

6.1.10 Incident management (ISMS controls A16)

Information security incidents, improvements, opportunities and feedback are booked and handled according to documented practices. Processes vary by criticality whereby critical events are handled immediately and low priority events are handled in regular information security group meetings. All persons related to service delivery are aware of incident management practises.

6.1.11 Business continuity (ISMS controls A17)

Sympa's business continuity is focussed on Sympa HR information security and service continuity. Identifying continuity risks and opportunities form the most critical part of Sympa's ISMS. Continuity is ensured with careful planning, reviews and regular third-party audits.

Sympa HR service continuity planning is based on high-availability design and fully redundant infrastructure.

6.1.12 Compliance (ISMS controls A18)

Compliance with applicable laws, regulations, authorities' guides and contractual requirements. Special attention is paid to intellectual property rights and regulations related to handling personally identifiable information (PII).

Compliance in information security is reviewed regularly by an independent third party.

7 Technology

The service is delivered as SaaS (Software as a Service) as a multitenant environment. The supplier is responsible for the information security and maintenance of the servers, the network and software, for system performance, availability and control, and for backups, updates and recovery from possible errors.

The system uses mainly Microsoft technologies (e.g. IIS, MS SQL, .Net) but is not limited to those.

Server infrastructure consists of both physical and virtual servers as well as some cloud computing resources. Critical parts are redundant. Micro-service architecture is followed to some extent.

Main databases are SQL servers but document databases and file storages are also used when more appropriate. All data is stored encrypted.

C# is the most common language in backend development. Frontend development is done with standard HTML, JavaScript and CSS with the help of frameworks and libraries like Marionette, Backbone.js and Sass.

Third-party software components and an open source code are also utilised in the application, where applicable.

7.1 Client-side requirements

The service is fully browser-based. No separate browser plugins or client applications are needed. Cookies and JavaScript have to be enabled in the browser.

As the service is developed by standard HTML, CSS and JavaScript languages, the services should be usable to full extent with any modern browser. We test all tools, features and processes with the most common browsers, such as Internet Explorer and Edge, Chrome, Firefox and Safari. Tests are performed with the latest desktop versions and patches (some exceptions to this when previous versions are still widely used). Up to date and more detailed information can be found from the Sympa support portal or on request from your Sympa contact person.

Data can be exported from the system to e.g. Excel or image files, or Word documents can be generated. Proper client application is required to open those.

8 Software Development

The development of the Sympa HR system is done mostly by Sympa employees in Finland. Selected partners within the EU are used for software development. All the production code is reviewed by Sympa employees, and external developers do not have access to personal data.

Agile methodologies are used, and the process is constantly being developed.

For quality assurance, a separate testing team is in place. In addition, test-driven development, automatic testing and code reviews are being used.

8.1 Updates, maintenance, and release cycle

It is important to address a distinction between updates (of the software) and releases (of new features). As Sympa HR is a SaaS product, Sympa is responsible for updating the Sympa HR software to the latest version, and there is no need for the customer to take any action. Updates, whether there are any new features or not, are included in the SaaS fee.

If the update contains new features affecting the end users significantly, the customer can usually dictate when the new feature is enabled (released) in their Sympa HR solution. There are two options as to how a new feature is enabled: either by the customer's administrator directly or by request from the Sympa support service. In both cases, the customer decides on the actual schedule. Thus, the end user experience will not change unexpectedly or at an inconvenient time. If the service and end user experience are directly affected by the update, the update is informed in a timely manner.

If the update contains any bug fixes or similar improvements, they are effective immediately once the update has been performed.

In general, updates are done without affecting the service. Only a few updates affect the availability of the service. If an update will lead to service downtime, the customer is informed about the update in advance. Updates are carried out outside (European) business hours or on weekends. This also applies to maintenance breaks.

Information about the updates and new features is delivered by email to the customer's contact persons and/or in our customer portal. Planned maintenance breaks are also visible to end users in the Sympa HR login page.

Because the customer decides on the actual schedule when new features are brought into use, and because of our agile development methods, there is no pre-defined release calendar. Our aim is to release new features as often as possible. The customer can then decide on the actual schedule with regards to their Sympa HR solution. New features become available, on average, every other month. This, however, depends on the scale of the features being implemented.

Confidentiality. The service description serves as an example of the service offered and a basis for modelling cooperation. No information included in this document may be disclosed to third parties or utilised for the development purposes of other suppliers.

This document describes the operations of Sympa at the time of documentation. Sympa reserves the right to further develop its operations and amend the services, technologies and methods described in the document without a separate notification.