Labforward GmbH
Elsenstr. 106, 12435 Berlin, Germany
www.labforward.io

Contact Labforward Team
contact@labforward.io
+49 (0)30 / 91572642

White Paper:

How Labforward protects personal data in compliance with the GDPR

By Yannick Skop

How Labforward protects personal data in compliance with the GDPR

Table of Contents

Introduction

When the General Data Protection Regulation (GDPR) came into effect in 2018, many companies were left unprepared. A 2017 survey conducted by Marsh & McLennan of over 1300 executives showed that only months before the GDPR came into effect, only 8% of respondents felt they were fully compliant with the upcoming changes. That number undoubtedly improved somewhat by the May 2018 deadline, but this survey result does speak volumes about the lack of preparedness across the board when it comes to data privacy.

Even more interesting is the correlation that was found between GDPR preparedness and cybersecurity preparedness:

> Companies that were partially or fully ready for the GDPR were more than **three times more likely to adopt cybersecurity measures**.

Why is this worth highlighting?

It is true that protecting the personal data of employees should be a top priority for every organization. Pharmaceutical companies, universities and other R&D organizations in particular, have even more reason to care about the data protection practices of their software vendors, as they also care a lot about protecting their scientific data (including but not limited to valuable intellectual property). When choosing a software vendor, you want to be confident in the vendor's commitment and capability to keep data safe, whether it is personal data or scientific data.

As a software provider that caters to scientists worldwide, including those in the European Union (EU), Labforward considers the introduction of the GDPR to be an important and positive development. On our journey to be GDPR-ready by May 2018, we did not just change a few legal documents and call it a day. Rather, we considered this to be an opportunity to strengthen our cybersecurity measures and ensure the entire Labforward team is laser focused on secure data management practices.

At Labforward, we have been focused on data privacy and security since the beginning, and we consider our commitment to implementing best-in-class data protection measures to be essential to our business. In this whitepaper, we will provide a transparent overview of the most important measures that are in place.

Executive Summary

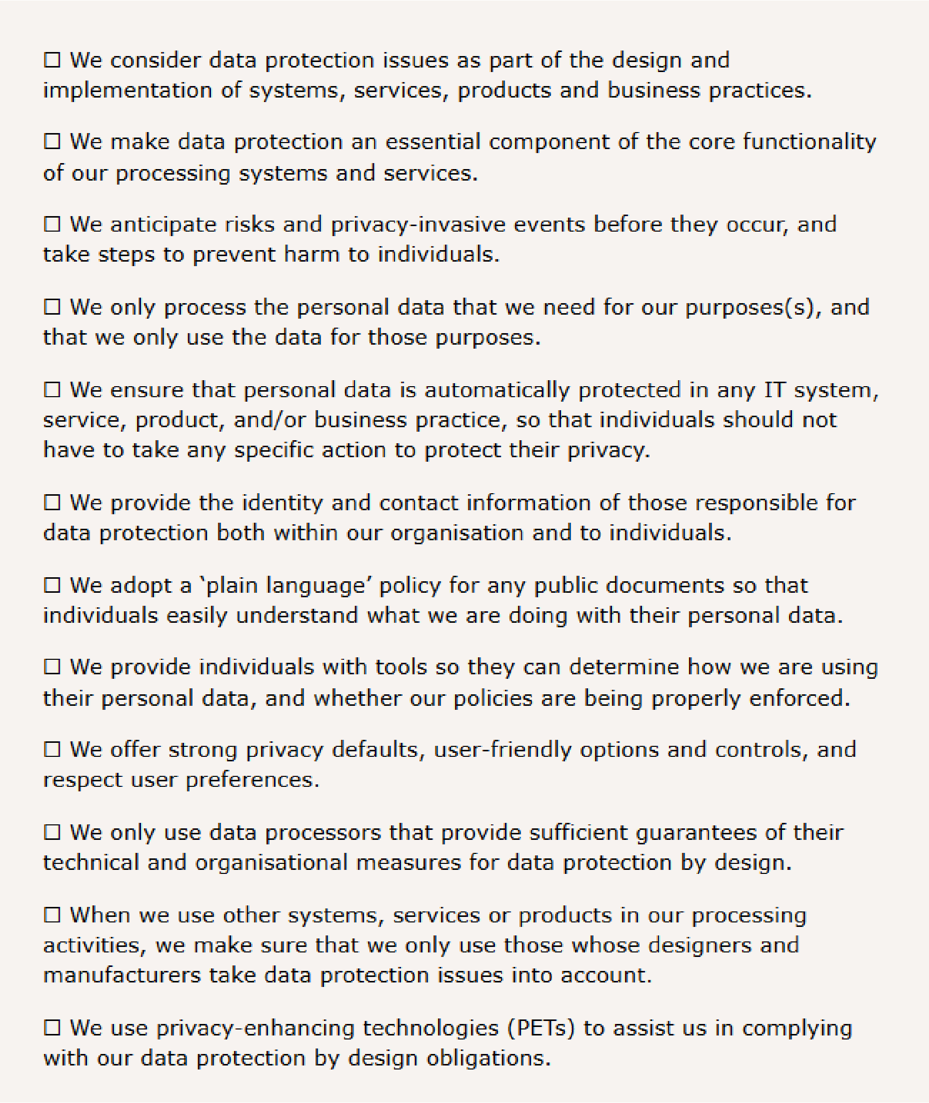
To ensure data protection and compliance with the GDPR, Labforward GmbH is:

1. Integrating data protection principles into our software development process (**Data Privacy by Design and Default**).
2. Offering customers the choice between two **GDPR-compliant hosting solutions**, either with a Public Cloud hosted in Germany, or On-Premises deployment of our software.
3. Making our privacy policy easy to understand and transparent, so anyone can figure out what kind of personal data is collected, stored, and used.
4. Implementing and documenting **technical and organizational measures** to protect personal data.
5. Offering a Data Processing Agreement to customers who choose our SaaS solution, in order to clearly regulate Labforward's role as a Data Processor.
6. Applying modern **software vulnerability management practices**, and transparently publishing security updates in our Security Center.
7. **Auditing our data protection practices** with an external provider to ensure we identify and correct any gaps.
8. Documenting our internal processes in our Quality Management System, training our staff and achieving **ISO 9001 certification** status.

1. Data Privacy by Design and Default

Data Privacy by Design and Default is all about considering data protection issues upfront. Software companies typically have no specific obligations about how to design and build products for optimal data protection performance, but in practice they need to consider the requirements of their customers who are the data controllers in order to be successful. Labforward is no exception here - when building our software solutions, our product & engineering team need to consider data protection from the onset.

The below checklist provides a good overview of how data protection is embedded in our software development processes (source: ICO):



☐ We consider data protection issues as part of the design and implementation of systems, services, products and business practices.

☐ We make data protection an essential component of the core functionality of our processing systems and services.

☐ We anticipate risks and privacy-invasive events before they occur, and take steps to prevent harm to individuals.

☐ We only process the personal data that we need for our purposes(s), and that we only use the data for those purposes.

☐ We ensure that personal data is automatically protected in any IT system, service, product, and/or business practice, so that individuals should not have to take any specific action to protect their privacy.

☐ We provide the identity and contact information of those responsible for data protection both within our organisation and to individuals.

☐ We adopt a 'plain language' policy for any public documents so that individuals easily understand what we are doing with their personal data.

☐ We provide individuals with tools so they can determine how we are using their personal data, and whether our policies are being properly enforced.

☐ We offer strong privacy defaults, user-friendly options and controls, and respect user preferences.

☐ We only use data processors that provide sufficient guarantees of their technical and organisational measures for data protection by design.

☐ When we use other systems, services or products in our processing activities, we make sure that we only use those whose designers and manufacturers take data protection issues into account.

☐ We use privacy-enhancing technologies (PETs) to assist us in complying with our data protection by design obligations.

2. GDPR-compliant hosting options

Labforward customers can choose between two hosting options for our software solutions:

1) Using our Cloud solution, which means we take care of all the hosting, deployment and updates to the server. When customers choose this option, they assign Labforward as their data processor.

   Labforward uses Amazon Web Services as its cloud provider, and has selected the eu-central-1 region (Frankfurt) to run its workloads. This means that your data is processed, stored and backed up in the EU, which is critical for GDPR compliance. AWS is an extremely secure cloud service which is regularly certified for compliance & security standards such as ISO 27001.

2) Using our On-Premises solution means that you are in full control of how your data is hosted and protected. In this case, Labforward does not act as a data processor and the responsibility for installing the latest updates of the software and performing regular backups sits with your IT team.

So which option is more secure, Cloud or On-Premises? We remain agnostic on this front, both options are secure with the right setup, and it all boils down to a matter of preference in the end. If your organization has an experienced and well-resourced IT team, and it is important that you are able to customize server configurations and exercise full control over your security measures, then On-Premises might be a good option for you. Alternatively, if these customization and control requirements do not necessarily apply to you, then you'll benefit from faster security updates and dedicated application monitoring provided by Labforward at no extra cost. Whatever hosting solution you choose, Labforward is here to support you.

3. Transparent and easy-to-understand Privacy Policy

How often do you see a privacy policy that can easily be read by 8th grade students? That is exactly the goal we set for ourselves when writing our privacy policy. Privacy policies should be easy to understand. Completely transparent, and written for the users of the software, not for lawyers.

The most important sections in our privacy policy score an 8.8 on the "Flesch–Kincaid" reading grade level. This means that it was written in plain English, and can be easily understood by 13- to 15-year-old students.

Moreover, we created a table of content for our privacy policy so that users can easily pick and choose the topics that they are most interested in. No more endless scrolling!

Table of Content

1. Identity of Labforward
2. What information do we collect?
3. What do we use your information for?
4. Legal basis
5. How do we protect your information?
6. Do we disclose any information to outside parties?
7. Third party links
8. Where do we store the information?
9. Access, data portability, migration, and transfer back assistance
10. Request for rectification, restriction or erasure of the personal data
11. Data retention
12. Accountability
13. Cooperation
14. Your consent
15. Changes to our privacy policy
16. Complaint

4. Technical and Organizational Measures

Labforward implemented several data protection measures in line with the requirements of Article 32 of the GDPR. This includes making sure that we employ an appropriate level of protection of personal data, avoiding unauthorized access to such data, while continuously monitoring and evaluating the reliability of these procedures.

a. Physical access control

Measures to prevent unauthorized persons from gaining access to data processing systems with which personal data are processed or used:

- Keys / key allocation
- Door security (electric door openers, etc.)
- Visitor control, escort and briefing

b. System access control

Measures to prevent the use of data processing systems by unauthorized persons:

- Assignment of user rights
- Creation of user profiles
- Password procedures
- Authentication with username / password
- Assignment of user profiles to IT systems
- Automatic locking
- Individual user accounts for authorized users (not root)
- Use of anti-virus software
- Encryption of data carriers in laptops / notebooks

c. Authorization control

Measures to ensure that those authorized to use a data processing system can only access the data subject to their access authorization and that personal data cannot be unauthorized, read, copied, modified or removed during processing, use or after storage:

- Demand-oriented design of an authorization concept and access rights, as well as their monitoring and logging.
- Administration of rights by system administrator
- Number of administrators reduced to the bare minimum
- Password policy incl. password length, password change

- Logging of accesses to applications, especially when entering, changing and deleting data
- Encryption of data carriers
- Job assignment and logging only in written form via ticket system
- Automatic generation of log files, where technically possible and reasonable, as well as evaluation of these logs in case of suspicion.

d. Transmission control

Measures to ensure that personal data cannot be read, copied, altered or removed without authorization during electronic transmission or while being transported or stored on data media, and that it is possible to verify and determine to which entities personal data is intended to be transmitted by data transmission equipment:

- No physical storage or transport of personal data.
- Logging of logins
- Encryption and tunnel connections (SSL, VPN, opt.)

e. Input control

Measures to ensure that it is possible to verify retrospectively whether and by whom personal data have been entered, modified or removed in data processing systems:

- Logging of commissioned database changes
- Proof of commissioning and successful processing in the ticket system
- Assignment of rights to enter, change and delete data on the basis of an authorization concept.

f. Order control

Measures to ensure that personal data processed on behalf of the customer can only be processed in accordance with the customer's instructions:

- Selection of the contractor under due diligence aspects (in particular with regard to data security).
- Prior review and documentation of the security measures taken by the contractor
- Written instructions to the contractor (e.g. by order processing agreement)
- Contractor has appointed data protection officer
- Ensuring the return/destruction of data after completion of the order
- Obligation of employees to maintain data secrecy in accordance with § 5 BDSG
- Control of data security precautions

g. Availability control

Measures to ensure that personal data is protected against accidental destruction or loss:

- Creation of a backup & recovery concept
- Testing of data recovery
- Creating a disaster recovery plan
- Keeping backup data in a secure, off-site location
- Avoiding single point of failure as the fundamental concept of all infrastructure
- Monitoring of infrastructure systems and deployments

h. Separation requirement

- Measures to ensure that data collected for different purposes can be processed separately.
- Separate development, test and production data processing
- Logical client separation
- Definition of database rights
- Authorization concept with definition of access rights

5. Data Processing Agreement

A DPA is a legally binding agreement that is entered between the data controller and the processor. It regulates the scope and purpose, as well as the relationship between the controller and the processor. In our case, our customers (research organizations) who choose to host their research data with Labforward's cloud solution, are data controllers who contract with Labforward as a data processor.

Why is a DPA important? The GDPR requires data controllers to ensure the protection of personal data they handle. If data controllers decide to outsource certain data processing activities, they must be able to demonstrate that their suppliers provide sufficient guarantees to protect the data and act in a GDPR compliant manner.

Signing a DPA achieves the above goal, provided that the data processor has indeed implemented sufficient technical and organizational measures (see section 4). Make sure to check that your data processor includes the following three annexes to the agreement:

1. Nature and scope of the data processing
2. Data security measures
3. A list of approved subcontractors

Labforward's DPA can be accessed here (EN | DE) and are part of our Cloud General Terms and Conditions (EN | DE).

6. Software Vulnerability Management

Vulnerability management refers to the practice of identifying, classifying, prioritizing, remediating, and mitigating security risks in software applications. This is of course a really important part of protecting personal data.

Labforward addresses this topic in multiple ways, of which we would like to highlight the following two approaches:

1. Through the use of **Automated Application Scanning** tools, we continuously test our software for possible security threats. These tools scan our applications not only for the Top 10 Web Application Security Risks (OWASP Top 10), but also for SQL injections, vulnerabilities behind authentication, input sanitation problems, SSL, CORS and encryption misconfigurations, and many more.
2. We also strongly believe in **Coordinated Vulnerability Disclosure** (CVD) as proven industry best practice to address security vulnerabilities. Through a partnership between security researchers and vendors, CVD ensures vulnerabilities are addressed prior to being made public. To prevent unnecessary risk to customers, security researchers and vendors do not discuss the details of reported vulnerabilities before an update is available.

Whenever we find vulnerabilities and fix them, we will be transparent about this with our customers and post an update in our Security Center.

7. External Audit

A data protection audit is a voluntary check of a company's data protection compliance. It is used to determine the compliance of the company with regard to the collection, storage and transfer of personal data. Such an audit includes interviews with employees, document reviews and examinations of the systems and processes.

During a data protection audit, secondary processes are also checked in addition to the core processes in operation. These are processes in the purchasing, sales, human resources, finance and IT departments in which personal data is processed.

Based on the results, measures are then suggested and recommendations for action made that should lead to an ideal target state in the company.

Labforward has engaged Dataguard GmbH, a leading data privacy & information security company, to conduct this external data privacy audit. The audit focused primarily on four areas:

1. General data protection (ex. the collection and processing of data, duty to provide information, etc.)
2. Subsequent data processing (ex. access rights to the data collected, programs used, etc.)
3. Passing on the data internally and to third parties (ex. processors, tax consultants, affiliated companies, etc.)
4. Security of the information (ex. technical precautions taken to secure the rights of those affected)

Together with the auditor, Labforward then developed an action plan with specific measures to keep improving our data protection processes.

8. ISO 9001 Certification

As of November 2021, Labforward is proud to be an ISO-9001 certified company. You can find a copy of our certificate here.

What does it mean to be ISO-9001 certified, and what impact does it have on our data protection compliance? ISO 9001 is a standard that sets out the requirements for a quality management system, which in turn is a way of defining a company's processes to help it meet its objectives and ensure customer satisfaction. This includes all the important data privacy processes.

Specifically, we took the following steps to ensure data protection best practices are followed at Labforward within the context of our Quality Management System (QMS):

1. **Creation of our QMS**
    a. Identifying and mapping out our core business processes, including those that involve personal data.
    b. Documenting all relevant policies, processes and work practices with the involvement of employees.
    c. Formally approving all documents and implementing version control.
2. **Implementation of our QMS**
    a. Ensuring procedures are being performed as described in our documentation.
    b. Properly training employees for the tasks they are performing through our e-learning system.
    c. Creating effective reporting systems to cover inspection, testing, corrective actions, preventive actions, management review meetings, etc.
    d. Continuously monitoring the effectiveness of our processes through the use of measurable data (where possible).
    e. Reviewing and taking action to improve in the areas required.
3. **Verifying that our QMS is effective**
    a. Conducting internal and external audits and reviewing the processes and system for compliance and effectiveness. This includes the interviewing of staff and looking at sample records.
    b. Identifying and reporting strengths and weaknesses of the management system.
    c. Taking corrective or preventive action as required.

Conclusion

At Labforward, we believe that we can only succeed in becoming a world-leading laboratory software company when we protect our customers' data. We will spare no effort to make sure we:

1. Consistently meet or exceed our customers' expectations with regards to excellence in data protection.
2. Respond to challenges by acting immediately and decisively, thereby improving our service delivery, company resilience, and customer satisfaction.
3. Identify, report, investigate and resolve all nonconformance and take action to prevent recurrence.
4. Evaluate continuously our internal Quality Management System, including our data protection policies and processes, and implement across all functions which impact the quality of our products and services in terms of personal data.
5. Educate and train our people to continually improve their skills, awareness and knowledge of data protection to foster core values in quality excellence and practices.
6. Uphold regulatory compliance including an ongoing review of statutory obligations, standards and codes of practice that apply to our business.
7. Maintain and monitor a culture that supports all of these objectives.

If you have any specific questions about how we protect your data, please feel free to contact our dedicated email address: dataprotection@labforward.io