Data Protection Policy

Effective: 16 December, 2022
Version: 3.0

SCOPE

The Scope of this policy is to:

- Describe how Camurus' employees should contribute to ensure compliance with data protection legislation; and
- Allocate roles and responsibility for data protection.

OVERVIEW

Camurus AB and its subsidiaries ("**we**"/"**Camurus**") are committed to ensure compliance with data protection legislation as part of good corporate governance and a sustainable approach to business. This Camurus Data Protection Policy (this "**Policy**") has been adopted to describe how Camurus works to ensure compliance with data protection legislation and to allocate responsibility within the organization regarding data protection and privacy. The Policy is intended to serve as a framework document, and is supplemented by clearly defined guidelines (1,3,5), with procedures and routines for compliance with data protection legislation, and templates (2), all of which are available via the Legal page on Camurus intranet.

This Policy, together with its supplementary documents, is based on the General Data Protection Regulation (EU) 2016/679 (the "**GDPR**").

This Policy applies to everyone within Camurus – all employees, managers and executive officers, the Board of Directors (which are included in the term "employees" for the purposes of this Policy), as well as any consultants and contractors (as regulated by contracts) who may process personal data in the course of conducting business on behalf of Camurus.

In accordance with the GDPR, Camurus has appointed a Data Protection Officer (DPO) who can be contacted by all employees at privacy@camurus.com. The DPO's main responsibility is to assist the organization in all issues relating to the protection of personal data. Camurus DPO is always available to assist in implementation of local policies and routines, as may be necessary to fulfil legal requirements for data protection.

All employees are obliged to ensure that they are familiar with the contents of this Policy, including its supplementary documents, and understand their related rights and responsibilities. If you have any questions relating to this Policy, please contact Camurus' DPO.

ROLES AND RESPONSIBILITIES

Role	Responsibility and Obligations
Data Protection Officer	• Establish, maintain and archive this Policy and supplementary documents • Ensure communication of this Policy and supplementary documents to the whole organization and offer training in GDPR compliance, as needed • Act as Camurus' DPO pursuant to the terms of the GDPR (including the tasks listed in Article 39) • Make annual updates to this Policy, and, as relevant, to supplementary documents

Role	Responsibility and Obligations
Country leads/General Managers/Business Unit Heads	• Notify the DPO whenever there is a need for local routines and procedures compliant with local data protection legislation to be implemented, e.g. notify the DPO when there is a need amend existing templates and guidelines as appropriate to ensure compliance with national rules and regulations
All Employees	• Follow and respect this Policy and any supplementary document • Perform trainings assigned by the DPO

POLICY

Risk awareness

Data protection and privacy of individuals is an increasingly important topic and component in companies' compliance with applicable laws and regulations. Safeguarding individuals' privacy is key to ensure full compliance with applicable laws and regulations but also to ensure sustainable corporate activities. Companies which fail to comply with the provisions of the GDPR may be exposed to significant financial and reputational risks and sanctions. Camurus is fully committed to complying with the GDPR and any other data protection legislation as may be applicable to Camurus' business.

Scope, internal responsibility, organisation and reporting

Camurus has decided to base its globally applicable Data Protection Policy on the GDPR, as Camurus is based in Sweden with functions where personal data processing become relevant are based at the headquarters in Lund, Sweden. However, Camurus operates on a global scale and must always consider that it may be subject to additional (local and/or national) data protection regulations applicable depending on where Camurus operates its business. It is the responsibility of the respective management of each Camurus company to notify Camurus' DPO if they need assistance in ensuring compliance with this Policy and applicable data protection and privacy laws and regulations relevant for the Camurus company in question.

In particular, the DPO should:

- inform and advise the organization of their obligations under data protection law;
- monitor compliance of the organization with all legislation in relation to data protection, including audits, awareness-raising activities as well as training of staff involved in processing operations;
- provide advice in relation to data protection impact assessments and monitor performance;
- act as a contact point for requests from individuals regarding the processing of their personal data and the exercise of their rights; and
- cooperate with data protection authorities and act as a contact point for data protection authorities on issues relating to processing.

Key principles of the GDPR

The GDPR applies to companies located in the EU/EEA and in some cases also to companies located outside the EU/EEA, when processing personal data. Personal data is defined as any information directly or indirectly relating to a living individual and the word processing means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

The overall purpose of the GDPR is to protect the fundamental rights and freedoms of natural persons and in particular their right to protection of their personal data. Based on the key principles listed below, the regulation imposes obligations on companies that process personal data.

a) *Lawfulness, fairness and transparency* – The processing of personal data by a company must be justified on a legitimate basis. Furthermore, it must be clear for the individual that personal data related to such individual is being processed, the identity of the company processing such data and for what purpose.

b) *Purpose limitation* – The purpose for the processing of personal data must be specified, explicit and legitimate and the personal data may not be processed beyond this purpose.

c) *Data minimization* – The company processing personal data must ensure that the personal data processed are adequate, relevant and limited to what is necessary for the purpose.

d) *Accuracy* – The company processing personal data must ensure that the personal data processed are accurate, kept up-to-date and to take every reasonable step to correct inaccurate data or erase it.

e) *Storage limitation* – The company processing personal data must ensure that personal data are not stored for a longer period than is necessary for the purposes for which the personal data are processed, which means that companies processing personal data must have knowledge of its processing activities, established retention periods and/or periodic review processes.

f) *Integrity and confidentiality* – Personal data may only be processed in a way which ensures appropriate security and confidentiality of personal data and prevents unauthorised access (such as hacker attacks) or accidental loss of data.

g) *Accountability* – Companies processing personal data must be able to demonstrate that they are in compliance with the obligations set out in Sections a)–f) above.

GDPR compliance within Camurus

All activities

Camurus is committed to ensure compliance with the principles of the GDPR and the obligations they impose on companies processing personal data. To ensure such compliance, it is the responsibility of all employees to:

- Read and understand this Policy and supplementary documents (1, 2, 3, 5) in their daily work;
- Involve Camurus' DPO whenever questions related to privacy and data protection occur;
- Comply with reporting obligations set forth in Camurus GDPR Guidelines, and use the relevant GDPR templates as needed (for instance a consent form for Camurus to process certain personal data). All GDPR guidelines and templates are available via Legal page on the intranet);
- Perform training assigned related to privacy and data protection.

Research and Development

Camurus is engaged in developing new and innovative medicines and medicinal products, where clinical research and the conduct of clinical trials in humans to evaluate the safety and efficacy of products are important components of medicinal product development. Camurus will always conduct its research and development activities in compliance with applicable laws and regulations, including any applicable data protection regulation, and is committed to ensure that individuals participating in clinical trials are not exposed to unnecessary risks. All data from clinical research is recorded, handled and stored in compliance with applicable laws and regulations, including the Declaration of Helsinki governing research and development performance and international standards of good practices, such as GLP and GCP.

Individuals participating in Camurus' clinical trials as study subjects are always provided with information as required under the GDPR, including without limitation information on the processing activities and of their rights, prior to being enrolled in the trial through the Informed Consent Form. Any research staff involved in a clinical trial are also provided with information on how Camurus process their personal data and their rights under the GDPR. Furthermore, clinical research organizations (CROs), vendors and other third parties involved in any research and development project must sign contracts with Camurus where the allocation of responsibility as regards data processing is clearly defined.

All data from clinical trials is only stored and archived as explicitly required under applicable laws and regulations, with highest security measures and standards. Access to data is strictly limited. Storage periods are clearly defined through applicable legislation.

Each employee is responsible to ensure that Camurus' DPO is involved whenever a new research and development project involving humans, e.g. a new clinical trial, is initiated. Each employee involved in any research and development project involving the processing of personal data must comply with Camurus' GDPR Company Guidelines and use relevant templates and documents provided within the Camurus GDPR Templates.

Human Resources

Camurus has implemented routines to ensure compliance with the GDPR when it comes to processing of personal data of Camurus' employees, hired consultants and job applicants. Employees, consultants and job applicants are informed of their rights under the GDPR and are provided with such other information as is required under the GDPR when Camurus acts as the data controller. Furthermore, Camurus' HR department has clearly defined retention routines to ensure that personal data of employees, hired consultants and job applicants (current and former) are only stored and processed as long as necessary and required under applicable laws and regulations. Camurus' DPO is always involved when privacy questions arise within the HR department.

To the extent Camurus works with third party services providers within the HR, e.g. payroll service providers and recruitment firms, all such third parties are obliged to sign contracts with Camurus as may be necessary to ensure GDPR compliance. Camurus' DPO is always involved when engaging a new third party, to ensure the allocation of responsibility under the GDPR is clearly defined and relevant agreements are signed (e.g. Data Processing Agreements).

Each employee involved in the processing of personal data of employees, hired consultants or job applicants must comply with Camurus' GDPR Company Guidelines and must always involve Camurus' DPO whenever privacy-related questions arise within the HR function. Camurus GDPR Templates relevant for the HR function are to be used.

Product Safety and Quality

Patient safety is of highest priority for Camurus. To monitor products that are subject to research and development activities as well as products placed on the market by Camurus, Camurus has implemented internal policies and standard operating procedures to ensure product safety and quality. These procedures include reporting lines to monitor any adverse events, quality issues and new and unexpected safety signals.

To protect the privacy of individuals involved in any safety or quality reporting, Camurus has developed automated means of ensuring such individuals are informed of their rights under the GDPR, including having signed agreements with third party pharmacovigilance services providers designed to ensure full GDPR compliance, and, provides clear instructions on the data processing to be performed by such third party on behalf of Camurus. No information other than as clearly necessary under applicable laws and regulations is stored.

All employees working with product safety and quality must comply with relevant parts of Camurus' GDPR Guidelines and use Camurus GDPR Templates.

Agreements with third parties

All Camurus employees must use Camurus' standard email signature with privacy notice in any external communication, in order to always refer any business contact to Camurus' general privacy notice. This procedure ensures that any business contact interacting with a Camurus employee through email, which is the most common form of communication, is provided with such information on how its personal data is processed by Camurus.

It is the responsibility of all employees to involve Camurus' DPO when engaging a new business partner, service provider or other third party with whom an agreement is to be signed, in order to ensure that all aspects of the relevant data protection regulations are covered in the relevant agreement. Further details are provided in Camurus' GDPR Guidelines, and templates and documents can be found as part of Camurus GDPR Templates.

Media and Communications

For the purpose of providing information on Camurus' business, including raising awareness around different diseases and conditions, Camurus engages in various media and communication activities. For instance, patient testimonials are an important tool for Camurus to provide such information and Camurus is always committed to share information with any individual who may request information on Camurus' business (to the extent allowed under applicable laws and regulations). Camurus may therefore need to process personal data of various individuals and clear guidance on how to ensure GDPR compliance when engaging in media and communication activities have been defined in the Camurus GDPR Guidelines. For instance, individuals providing patient testimonials must always consent to their personal data being processed and individuals requesting information from Camurus are provided with privacy notices describing the data processing and their rights under the GDPR.

It is the responsibility of each employee to ensure full compliance with the Camurus GDPR Guidelines and know what documents to use and how to involve Camurus' DPO when working with media and communication activities and content.

Medical Affairs/Commercial

Camurus has implemented routines and guidelines applicable to all interactions with Healthcare Professionals (HCPs), Healthcare Organizations (HCOs) and Patient Advocacy Organizations (PAOs), designed to apply the highest standards of integrity and honesty and compliance with applicable laws and regulations, including GDPR. All HCPs are provided information as required by the GDPR for Camurus to process their personal data. For the purpose of reporting transfers of values as required by

the EFPIA Code, or applicable national laws, regulations or industry code, Camurus will ensure that GDPR requirements are adhered to, which, subject to local conditions, may include the provision of consent, or other legal grounds for processing.

Each employee interacting with HCPs, HCOs or PAOs must comply with applicable Compliance Company Guidance and must always involve Camurus' DPO to ensure a proper agreement, is signed before any HCP, HCO or POA is engaged to perform services for Camurus, and that the provision of privacy notice, and/ or the sign-off of consent, is covered for the engagement.

Furthermore, any interaction with individuals at events or conferences (whether remote or physically) must be made in compliance with applicable Company Guidances, to ensure that proper information on the data processing is provided to any such individual. Templates and documents are provided within Camurus GDPR Templates.

Personal data processed during whistleblowing and compliance investigations

Camurus system for whistleblowing reporting concerning suspected misconduct of Company Policies, Company Guidance, and applicable laws, regulations and industry code, provides secure reporting mechanisms, to ensure that the privacy of the reporter, and any person which is subject to the allegations of suspected misconduct, is handled in a confidential manner and in full respect of GDPR requirements (4). Camurus processing of personal data in relation to whistleblowing and compliance investigations is described in a "Notice to reporter", which is made available directly in the online reporting tool, and also via Camurus intranet.

POLICY COMPLIANCE

Personal Data Breaches:

Any personal data breach must promptly (within 24 hours) be reported to Camurus' DPO at privacy@camurus.com. The procedures for the further handling of personal data breaches, including reporting to relevant Data Protection Authorities, is described in the separate guideline "Personal data breach procedures" (5).

Suspected misconduct:

Reports of suspected misconduct concerning this Policy, or of applicable data protection and privacy laws shall be made to Camurus DPO, or through Camurus' whistleblowing system, which facilitate anonymous reporting and follow up. The whistleblowing system is made available via Camurus intranet and the corporate website. Confirmed misconduct could result in disciplinary action up to and including termination of employment. Camurus will not tolerate retaliation against anyone for reporting concerns in good faith.

ABBREVIATIONS AND DEFINITIONS

DPO	Data Protection Officer
GDPR	General Data Protection Regulation (EU) 2016/679
HCO	Healthcare Organization
HCP	Healthcare Professional
PAO	Patient Advocacy Organization

Personal data	Any information directly or indirectly relating to a living individual and the word processing means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
Personal data breach	Means a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to, personal data transmitted, stored or otherwise processed.