Position on Privacy, Data Protection and Data Ethics

1 Introduction

Chr. Hansen has an ethical and responsible approach to the use of data. This Position on Privacy, Data Protection and Data Ethics ("Position") describes the standards Chr. Hansen adheres to including Chr. Hansen's commitment to responsible and ethical use of data.

2 Scope

This Position applies to all data types handled by Chr. Hansen and to all aspects of the organization worldwide.

3 Chr. Hansen's commitment to data ethics

We seek to establish a strong culture of data ethics awareness and encourage employees and business partners involved in the use of data to raise concerns and ensure that use of data is always based on informed decisions guided by the principles set out in this Position.

4 Guiding principles for data ethics

The guiding principles for data ethics below set the ethical standard for how we use data within Chr. Hansen. The guiding principles apply in combination with other policies and procedures adopted by Chr. Hansen.

4.1 Lawfulness, Fairness and Transparency

All data shall be *processed lawfully, fairly and in a transparent manner*. Therefore, we collect and process personal data only when we have a legal basis for doing so and have informed the individuals in advance.

Our use of data must comply with applicable law.

We always focus on the human impact and potential harm that we may cause to individuals when using data. Our commitment to fair and transparent use of data also means that we must understand the effects caused by our use of data and ensure that

our use of data does not lead to discrimination or unfair restrictions of the rights and freedoms of individuals.

4.2 Purpose limitation

In our use of data, we always consider why the data was originally collected and whether any secondary use of the data is compatible with the fair expectations of the individuals or organizations that have provided the data. Secondary use and combination of data sets can provide powerful insights, but such use must always be balanced against the fair expectations of individuals and organizations involved and the trust that underlies any decision to provide us with data.

Personal data shall be *collected for specified, explicit and legitimate purposes and not further processed* in a manner that is incompatible with those purposes.

4.3 Data Minimization

Data shall be *adequate, relevant and limited to what is necessary* in relation to the purposes for which they are processed. Although we legally can collect and use data, we stay aware that the collected data may be useful in the future for new and unpredictable purposes that can pose risks or be harmful to individuals, communities and the general society. By minimizing data, we also limit the risk of creating unintended risks or harm in the future.

4.4 Data Quality

Data shall be *accurate* and, where necessary, kept up to date. Use of incorrect, inconsistent or untimely data can lead to misinterpretations and wrong decisions that may cause harm to individuals, communities and the general society. When using data, we always consider the completeness, consistency, uniqueness, accuracy, validity, and timeliness of the data we use and how we can identify and prevent potential adverse effects caused by insufficient data quality.

4.5 Storage Limitation

We are responsible for data in our possession, and we always need to balance our need for keeping data as part of our business processes against the fair expectations of individuals and organizations involved and the inherent risk that data may be used for unpredicted purposes.

Personal data shall be kept for *no longer than necessary*. When personal data is no longer necessary, all data shall be deleted securely in accordance with good practice deletion standards.

4.6 Security, Integrity and Confidentiality

Data shall be processed in a manner that *ensures appropriate security* in particular with respect to personal data that must be protected against unauthorized or unlawful processing and against accidental loss, destruction or damage. Therefore, Chr. Hansen has implemented appropriate technical or organizational measures and employees only have access to personal data on a strict need-to-know basis.

4.7 Accountability

We are responsible for data in our possession and accountable for how we use data. Therefore, we require robust governance of data usage in all parts of the organization. We are cautious that interpretation of data is affected by humans, culture, changing legislation and the tools we use to analyse data. Governance should encourage and facilitate an open dialogue about data ethical dilemmas.

The Global Privacy Officer must be involved when we engage with third parties to assist us with handling personal data to ensure that our standards are complied with throughout our supply-chain.

We shall be able to *demonstrate compliance* with the principles.

5 Training and Awareness

Training in privacy, data protection and data ethics is part of our compliance training, and we ensure relevant Chr. Hansen employees know what data ethical behavior entails and can navigate accordingly in a digitalized environment. Furthermore, all employees are required to make themselves acquainted with the rules and procedures on privacy, data protection and data ethics that apply to their functions.

6 Reporting Mechanism and Complaints

The Global Privacy Officer shall be notified in the event of a potential personal data breach or any other concern about a potential violation. Furthermore, all employees are encouraged to seek advice from their manager, Local Data Protection Responsible or Global Legal Compliance when in doubt regarding a privacy or data ethics compliance matter.

Global Privacy Officer: privacyofficer@chr-hansen.com.

7 Publication

This Position is available on C-Net and on the website www.chr-hansen.com.

This Position must be reviewed at least once a year.