Erasure policy

Policy for erasure of personal data

For every employee in:

Qmed Consulting A/S
Købmagergade 53, 1. floor
DK 1150 Copenhagen
CVR-nr.: 30564278

(”us”, ”we” or ”ours”).

This is version 1, updated the 18.08.2022

1. Introduction

1.1 This erasure policy (the "**Policy**") outlines the guidelines for how long we process personal data and how we erase it.

1.2 The Policy is formulated and made available to you for us to comply with the General Data Protection Regulation (2016/679 of the 27 April 2016) (the "**GDPR**"). We have chosen to make this Policy to demonstrate and document our time limits and methods for erasing personal data and to ensure a uniform approach for erasure.

1.3 We monitor and control that this Policy is complied with on an ongoing basis, including monitoring whether personal data is in fact erased and/or returned in accordance with this Policy. We also continuously review the Policy to assess any needs for changes, for example due to amendments in applicable law or other internal policies that affect the Policy.

1.4 The policy proceeds with a general section about erasure followed by a section about methods for erasing and returning personal data. Next, the specific retention periods are provided in separate sections, each of which may contain several items, e.g. section 4.1. These items will first state the personal data covered and then when they shall be erased. At the end of the policy, two short sections are provided, concerning the reservation of possible changes to the Policy and contact information for questions.

2. About erasure in general

2.1 Personal data may only be "kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed". This is a requirement under GDPR and it is therefore important that you follow our procedures and guidelines to ensure that erasure always happens in accordance with the applicable retention periods.

2.2 The retention periods may in certain cases be derogated from, e.g. to comply with law requirements or other legitimate interests like the Danish Bookkeeping Act, the Danish Limitations Act, an obligation arising from a guarantee, or other mandatory requirements. You therefore might have to follow another instruction which proceeds the Policy. As an example, we keep personal data if there might be non-statute-barred claims, provided that the continued processing of personal data is necessary to protect or submit the claim. Similarly, client contracts may specify the retention period, and how personal data shall be erased or returned. In addition, inaccurate personal data shall be erased or rectified immediately in accordance with the relevant procedures. It is therefore important to understand that the Policy is guiding in the sense that there may be deviations. When in doubt, you should contact your immediate manager.

2.3 Notwithstanding the provisions in the Policy, personal data may be stored in our backup systems in accordance with said systems' retention period. If personal data are to be recovered from backup, it shall be done in accordance with instruction from the immediate manager.

2.4 If we receive requests from data subjects concerning their rights under GDPR, erasure may also be relevant and needed. Such erasure based on data subjects' requests will follow

specific procedures for handling data subject requests and inquiries. Please direct any questions to the contact details provided at the end of this policy.

3. Erasure and returning methods

3.1 Personal data shall be returned or deleted in accordance with the relevant sections in this Policy. You shall always ensure that there is no exemption to the retention period before erasure is done. Always ask your immediate manager when in doubt.

3.2 Personal data in digital/electronic form shall be destroyed, demagnetised or overwritten in accordance with our procedures to ensure that personal data are erased effectively. Personal data may be stored on many different types of electronic media and it is therefore important that you ask your immediate manager when in doubt. For example, there may be personal data in desktop computers and in laptops, tablets, smartphones, USB flash drives, SD cards, external hard discs, routers, printers, fax machines and CD's.

3.3 When digital equipment needs repair it is important that you take precautions before you hand over the device so that any external repairer before, during or after the repair of your digital device does not copy or otherwise store the personal data on your device. You must therefore consult your immediate manager and any IT department to receive guidelines for safe and secure repair of digital device. In accordance with such guidelines, appropriate measures must be taken to ensure continued confidentiality of the information on the digital device. For example, as appropriate, it might be necessary to (i) create backups via the device and store them on a separate equipment, after which all content on the device is erased, (ii) delete any confidential information from the device, and/or (iii) have the external repairer sign a non-disclosure agreement and inform the repairer about the confidentiality of the personal data covered. It is therefore important that you always consult with your immediate manager and possibly consult your IT department before sending digital equipment to external repair.

3.4 Personal data in physical form shall be destroyed by shredding or other measures that ensure that unauthorised persons cannot read or access the information in any way. Personal data may be stored in many physical documents, and it is therefore important that you, when in doubt, ask your immediate manager before selling, reusing, leaving or trashing physical documents. For example, personal data may be found on loose paper, post-it notes and notebooks. Specific information about the retention periods for relevant types of personal data is given on the following pages.

4. Erasure of personal data as a data processor

4.1 In some cases, the Company will process personal data on behalf of a data controller and thus be data processor, cf. GDPR, Article 4 (8).

4.2 In these cases, the Company's erasure procedures will appear in an instruction in a data processing agreement, cf. GDPR, Article 28 (3) which will thus take precedence over this erasure policy.

4.3 If you need to know how and for how long the Company should keep personal data processed on behalf of a data controller and how to delete it, must therefore follow the data processing agreement, you will therefor need the specific data processing agreement rather than following this erasure policy.

5. Hiring process

5.1 **Motivational letters and applications**, including for example appendices, CV, references and recommendations, reasons for rejection, notes from job interviews etc., criminal records, personal data from social media such as LinkedIn, and health information. Retention periods: When the candidate becomes an employee, the employee's personal data from the application process are transferred/moved to regular HR management. Find more information under the section about HR management. When the candidate does not become an employee, the personal data is erased. Under Danish law, the personal data is as a general rule deleted, at the latest, 6 months after; (i) the position is occupied by another person; (ii) the candidate declines the job offer; or (iii) the candidate, after having accepted a job offer from us, terminates his or her contract. If the candidate consents to a longer retention period, we follow such period. Notwithstanding the above, specific reasons related to employment law may necessitate the continuous processing of the personal data. This may have different implications. For example, we may process the applications for a longer period to prove that there has been no unlawful discrimination in the selection process, when we consider this necessary. Similarly, it may be relevant to process the personal data for a limited period if a similar relevant position may become available during this period, or if another existing candidate opts out of the application process.

6. HR management

6.1 **Employment contracts, appendices and addendums**, including for example photographs, non-disclosure agreements, non-compete clauses, social security numbers written in the contracts, gender, and civil status. Retention periods: During employment, every version of the employment contracts, addendums and appendices, are kept and stored because they are considered necessary to keep in order to administer the employment. When the employment is terminated, the personal data is erased. Under Danish law, the personal data shall as a general rule be erased, at the latest, 5 years after the calendar year where the termination took place, provided that the personal data in the employment contracts is still relevant.

6.2 **Employee personnel files and registers**, concerning employment history, including for example job applications for other positions after the employment, promotions, warnings, relocations/redeployments, absence not due to sickness, examination certificates, certifications of qualifications, performance evaluations, personality tests, development plans, information related to executive/management development, contact information of nearest relatives and similar, photographs, travelling history, trade unions, and unemployment insurance fund. Retention periods: Employee personnel files etc. are used to administer our employee's employment. As a general rule, such personal data shall, at the earliest, be erased after the termination of employment, and when it is no longer relevant to keep them. During employment, every employee personnel files and registers are kept if it is relevant for the employment. The personal data in employee personnel files and registers

are deleted after the termination of employment. As a general rule, the personal data is erased after 5 years from the termination of the employment, unless disputes, inspections, audits or similar necessitates continuous processing in order to protect or submit a claim or similar. Photographs of employees are as a general rule deleted immediately after the termination of the employment, unless it is necessary to continually process them and as long as the legal ground for the processing remains, while specific assessments are needed concerning work-related injuries.

6.3 **Information regarding health**, including for example documentation concerning the absence of the employee related to sickness, reports about work-related injuries, including fit-for-work certificates and duration declarations, medical certificates or statements, etc. Retention periods: The personal data shall be deleted when it is no longer relevant. Because the processed data concerns health information which is a special category of personal data, a high degree of attention must be given in the ongoing assessment of whether the health information is relevant to store or process. During employment, personal data concerning health can as a general rule and at the utmost be processed for 5 years after the collection, on the condition that there is a relevant, fair, and legitimate purpose for the collection and processing during all 5 years. The personal data shall be deleted after the termination of employment. The personal data may only be stored after the termination of employment when it is strictly relevant and necessary to pursue legitimate purposes, e.g. to store documentation needed for a current or potential dispute relating to employment law when such personal data is needed to process the case. Under Danish law, this retention period will as a general rule be up to 5 years after the termination of employment because employmentrelated claims are time-barred 5 years after the occurrence of the circumstances leading to the claim. Specific assessments are needed in the case of work-related injuries so that the personal data is only stored to the extent it is necessary and relevant in each case.

6.4 **Activities related to training and education**, including for example supplementary training and re-education, certificates or other documentation for the completion of a course, educational programme, or other training. Retention periods: Personal data about such activities etc. shall be erased when they are no longer relevant. During employment, the personal data may be stored and processed in accordance with the purposes for which they were collected. This means that the personal data as a general rule does not need to be erased during employment. When the employment is terminated, the personal data shall be erased. Under Danish law, erasure shall as a general rule be done, at the latest, 5 years after the termination of employment.

6.5 **Logging** of IT equipment and systems and use of email and internet, for example in log files and audit logs. Retention periods: The personal data are deleted when it is no longer necessary to store them for security purposes or for monitoring performance or similar, and when any national rules about logging no longer require us to store them. Under Danish law, these personal data shall as a general rule be erased 3 years after the time of logging unless applicable legislation specifically regarding logging predicts otherwise. Logfiles on the employee's electronic equipment are erased, at the latest, 3 years after the time of logging.

6.6 **Information related to vacations** such as the right to holiday bonus. Retention periods: Personal data related to vacations are erased when they are no longer relevant to store for accounting purposes, and when there are no other relevant purposes to pursue with the storage, e.g. documentation relevant to potential disputes relating to employment law. Under Danish law, the personal data shall as a general rule be erased 5 years after the end of the financial year in which the personal data was collected.

6.7 **Administration of salary** and documentation for paying salaries, e.g. working hours, registration of working hours, pension payments, bonus allotments, bank account information, payslips with personal data such as name, address, social security number, time of employment, holidays and extra holiday entitlements, pension information, labour market contributions, types of income, types of taxes, specifications of entitled payments due to travelling, national labour market supplementary pension, tax allowances, participations in lunch schemes. Retention periods: The personal data shall be erased when they it is no longer necessary for accounting purposes and when there is no longer another relevant purpose for storage, e.g. documentation relevant to potential disputes relating to employment law. Under Danish law, the personal data shall as a general rule be erased 5 years after the end of the financial year in which the personal data was collected.

6.8 **Reports to tax authorities** and documentation for salaries of the employees. Retention periods: The personal data shall be erased when it is no longer necessary to process for purposes of accounting or tax, and when there is no longer any other relevant purpose for storage, e.g. documentation relevant to potential disputes with tax authorities or similar. Under Danish law, the personal data shall as a general rule be erased 5 years after the end of the financial year in which the data was collected.

6.9 **Notifications of work-related injuries**, including name, address, contact information, health information etc., which do not relate to employee personnel files. Retention periods: The information is stored, partially to comply with law requirements and partially to handle the claims developments optimally. Under Danish law, the filings and its appendices, including the personal data contained therein, shall as a general rule be deleted 5 years after the injured person become aware of the claim. However, you need to perform an individual and specific assessment of the need for erasure as there may be many other factors that can substantiate continued storage of personal data in relation to work-injuries. Erasure of personal data regarding workinjuries shall always be done in accordance with instructions from your immediate manager.

7. Professional relations

7.1 **Regular information related to professional relations such as customers, members, consultants and partners** like name, phone number, email address, address, company name, job position, invoicing and accounting vouchers and economic information, state of bills, purchase history, information related to guarantees, etc. Retention periods: The personal data shall be erased when it is no longer necessary for purposes of accounting or tax, and when there is no longer any other relevant purpose for storage, e.g. documentation relevant to a current or potential dispute. Under Danish law, the personal data shall as a general rule be erased 3 years after the end of the financial year in which the personal data was collected while information related to bookkeeping are erased 5 years after the end of the financial year. Information relating to guarantees may, however, be kept for 10 years after the guarantee was made, and 3 years after any potential claim made during the guarantee period.

7.2 **Personal data in CRM systems and similar**

Retention periods: It is assumed that CRM systems are only used to process information about customers/clients, members, partners, consultants and similar professional relations. In existing customer or partner relationships, the personal data may be stored for as long as

there is a customer or collaborator relationship, and for as long as there is a relevant purpose to keep the relationship. The personal data shall be erased when the customer or partners relationship is terminated. Under Danish law, the personal data may as a general rule be stored for 3 years after the termination of the customer or partner relationship on the condition that the storage is relevant, for example to document the course of the customer and partner relationship or because of any potential case manager responsibility or claims. When personal data is processed in relation to ongoing customer or partner relationship, for the use of delivery, advisory or other processing of individual cases or incidents for the customer or partner, the personal data shall be erased 3 years after the termination of each individual case, unless there is a fair and legitimate purpose to process the personal data via the customers general and ongoing relationship. If special categories of personal data are processed in connection with an individual case, strong reasons are needed to justify the continuous storage and processing of personal data after 3 years after the termination of the customer case.

7.3 **Contracts** including case material and appendices etc. and the contained personal data like contact information, descriptions, pictures, signatures etc. Retention periods: Contracts shall not be erased during the period and term of the agreement included in the contract unless exceptional circumstances arise. When the contract term is finished, the contracts shall not be deleted until after we are sure that the contracts are no longer in any way relevant or necessary in order to document a potential claim or dispute. Contracts and the contained personal data shall only be erased based on instruction from your immediate manager.

8. Emails

8.1 Employee email accounts and emails

Retention periods: Under Danish law, all emails, including the inbox, deleted items, attached files, sent items and archive, which contain personal data, shall as a general rule be erased, at the latest, 1 year after the termination of the employment. During the employment, the employees shall preferably store business-relevant emails in an archive, for example dedicated Outlook folders, and delete other emails that are not business-relevant. Business-critical information and documentation may occasionally be stored in employee emails. Such business-critical information and documentation will be covered by a longer obligation of retention and may be stored in the emails for as long as there is a legitimate purpose with storage. Such emails shall as a general rule preferably be stored in an archive, separate from the rest of the “general” emails. Furthermore, it may be necessary to process email accounts for storing information contained in emails or for the purposes of migrating the information to other data media. In addition to the above, there may be many specific and fair reasons for storing emails and the contained personal data for a longer time than 1 year after the termination of employment and such a continuous processing may therefore take place based on a specific assessment and identification of relevant and fair purposes for the continuous processing and storage. Emails clearly marked ”private” in accordance with our policies shall not be stored longer than strictly necessary and shall not be migrated onto other data media after the termination of employment.

9. Marketing

9.1 **Recipients of marketing**, for example names, emails and phone numbers of people and consents for direct marketing. Retention periods: Information about the recipients of marketing material is stored in the period necessary for establishing and maintaining a future legal contact or marketing to the recipients. The personal data shall be erased immediately when they are no longer necessary, or when the recipients withdraw their consent they have provided and there is no other valid basis for processing.

10. Website

10.1 **Website visitors**, meaning, for example, cookies and other tracking technologies, behavioural profiles, etc. Retention periods: We refer to our separate policies on this topic, e.g. our cookie policy.

11. Internal material

11.1 This Policy does not regulate retention periods for personal data about internal material.

12. Changes to this Policy

12.1 We reserve the right to update and change the Policy. If we change the Policy, the date and version at the top of this document will change. In the case of substantial changes, we will tell the relevant employees directly.

13. Contact

13.1 If you have questions or comments to this Policy, you can always direct them to gdpr@qmed-consulting.com.