Appendix to Internal Integrity Policy
Last updated 15 mars 2021

Erasure routines for personal data

Introduction

This document, which is an appendix to our **Internal Integrity Policy**, describes the routines to be followed in the KAMIC and Amplex Groups for erasing personal data in order to ensure that we comply with the requirements for minimising storage and erasure set out in the General Data Protection Regulation (**GDPR**).

The underlying principles of GDPR state among other things that we shall strive to minimise the amount of personal data we collect, ensure that the information we hold is correct and not store the information for longer than necessary. In addition, for all processing of personal data there must be a legal ground for the specific processing we intend to carry out.

This document, however, only covers erasure routines and does not of itself provide sufficient information on how we shall process personal data. A more comprehensive description of what GDPR means for our processing of personal data can be found in the Integrity Policy. Employees of KAMIC Group and Amplex companies are obliged to take note of this policy which is available on the KAMIC Group intranet, from KAMIC Group's Head of Corporate Communications and from all business area and company managers.

NB:

The erasure routines are divided up based on two categories of individual whose information we process, a) **personal data about customers, suppliers and other external parties**, and b) **personal data about employees**. This division is motivated by the fact that there are many of us who need to be aware of the erasure routines for customers, suppliers and other external parties at the same time as there are only a few types of personal data and the routines are therefore relatively uncomplicated. For personal data about employees the opposite applies – there are only a few of us who need to know when these should be erased but we process a large amount of different personal data about our employees and the routines are therefore more complex.

Consultants and trainees are also considered as employees.

When the term erased is used in these routines, under certain circumstances an adequate alternative may be to anonymise the personal data.

There are many laws which regulate how companies and employers may conduct and administer their business and which also govern what personal data the company needs to process and how long these may be stored. In Sweden, this is governed for example (but not exclusively) by the Employment Protection Act, the Work Environment Act, the Working Hours Act, the Annual Leave Act, the Discrimination Act, the Co-determination in the Workplace Act, the Accounting Act, the Sale of Goods Act as well as through taxation legislation. **The erasure routines described in this document are developed to satisfy Swedish requirements and legislation**. In other countries where we have operations there is often corresponding legislation but there might also be differences in regulations for storage times, and also other national laws which govern processing of personal data in the country concerned.

In the event of changes to GDPR or other applicable data protection legislation, these erasure routines may be revised. The routines can also be revised on the initiative of the managements of KAMIC Group or Amplex.

pp Managements of KAMIC Group and Amplex

Håkan Lundgren
Head of Corporate Development & Communications

ERASURE ROUTINES FOR PERSONAL DATA ABOUT CUSTOMERS, SUPPLIERS AND OTHER EXTERNAL PARTIES

Almost all of us process personal data to some extent in our work and therefore need to know how these personal data can be stored and when they must be erased. Some categories of staff, however, process personal data more often and as an essential part of business operations. These include *account managers, purchasing managers, as well as employees in IT administration, accounts/bookkeeping, communication and marketing*. These routines therefore especially affect those of you who work in one of the above areas.

- In our business system there is personal data about contacts at our customers and suppliers and to some extent at other cooperation partners. Account managers, salespersons and purchasing managers are responsible for keeping "their" personal data up to date and ensuring that incorrect/out-of-date information is erased. Updates should be made on an ongoing basis but at least once a year *a coordinated and structured inventory* should be made of the registers of persons that we maintain. Business area managers are responsible for planning and initiating such coordinated inventories in their respective companies.

- What is stated above regarding ongoing updates and annual reviews applies regardless of the platform and/or storage medium on which the personal data is saved. It therefore includes customer and supplier registers on an individual's own hard drive, in an own or shared folder on the company's server as well as on a mobile phone or tablet.

- Personal data about customers and suppliers with which we no longer have any business relationship must be erased. As a rule, if we have not had any interaction (= dialogue) for three years the information should be erased. Note however that personal data should be saved if it is needed in order for us to perform any legal obligation that we have towards the customer/supplier.

- Personal data about *potential* customers stored in the CRM system and also on other platforms must also be kept up to date and erased according to the same routines as above (i.e. annual reviews and stored for no more than three years if we have not had any interaction). Account managers and salespersons are responsible for erasing "their" information.

- Invitation lists and lists for marketing mailshots must always be processed with attention to the GDPR rules on legitimate interest and consent. In short these mean that we have the right to use a register of persons for sending marketing and information material to existing and potential customers. At the same time, at an appropriate place in these mailshots we must inform the recipient that he/she has the right to be omitted from future mailshots and provide a simple method for this such as a "deregister me" link (if transmission was by email) or a checkbox "Yes, please for continued information" which must be actively checked (if contact was via a web tool).

- Those registers of persons that are used for mailshots may not therefore include anyone who has declined mailshots from us (and they must of course be otherwise kept up to date). It is up to the account managers, salespersons and marketing managers to make sure this happens.

- Media lists which are used for sending information in the form of press releases to journalists, industry forums and similar must be kept up to date by communication and marketing managers. Personal data which has not been used for three years must be erased.

- Personal data about customers and suppliers in accounting material such as vouchers, contracts, invoices and other legal documents must according to the Accounting Act be saved for seven years from the end of the calendar year in which the financial year ended (i.e. seven years + current year). Thereafter, all *personal data* must be erased (other information can be kept longer if needed). This applies to both accounting information stored electronically in our business system and in physical binders and similar. Accounts staff are responsible for erasure.

Personal data in the email system is a separate chapter where GDPR makes demands on storage and erasure which mean that many of us will need to think and act somewhat differently from what we are used to. The company's email system is used by almost all employees which means that these new requirements apply to *almost all of us*. To comply with GDPR at an acceptably high level in this area as well, we need, in addition to erasure routines, some rules for *using* email.

- When we receive or open a new email message we should immediately assess whether we need the message for our work or not. If the answer is clearly no, then the message should be erased.

- When we send email we must be restrictive in copying in recipients. Email should only be sent to those who really need the information for their work.

- We must be careful about forwarding email without having read the entire message first. Perhaps certain information (with or without personal data) must be removed before forwarding.

- Everybody must at least once a year go through their archived email and clean out those that are no longer relevant or for some other reason no longer needed. This also applies to own distribution lists, own address book and autocomplete functions. Note that address books can also be in mobile phones and tablets.

- Email which is in the deleted items folder (which was once deleted) as well as the email in the sent items folder should be cleaned out more frequently, at least quarterly. Sent email which is to be kept must be archived in a dedicated folder "saved/archived".

- The company's shared address book must be kept up to date by the IT administrator.

Erasure routines for email upon termination of employment

These routines are described below under Erasure routines for personal data about employees.

Summary of erasure routines for personal data about customers, suppliers and other external parties			
Document type/subject	**Storage place**	**Erasure routine**	**Responsible**
Contact persons at customers, suppliers	Business system (e.g. Jeeves) but also other storage platforms (own computer, company's server, mobile phone, etc.)	• In general, personal data must be kept up to date on an ongoing basis. • A coordinated review of personal data must be made at least once a year. • If there is no ongoing business relationship and we have not had any interaction with the person in the past three years, information must be erased.	Account manager, salesperson, purchasing manager. Business area manager is responsible for making an annual inventory.
Contact persons at potential customers	CRM system and other platforms	• A coordinated review of personal data must be made at least once a year. • If we have not had any interaction with the person in the past three years, information must be erased.	Account manager, salesperson
Lists for sending invitations and other marketing	CRM system and other platforms	Must be kept up to date on an ongoing basis. May not contain persons who have declined mailshots.	Account manager, salesperson, marketing manager
Media lists	Own folder on the company's server	Must be kept up to date on an ongoing basis. If nothing has been sent for three years, the personal data must be erased.	Information and marketing managers
Accounting information (bookkeeping)	Business system and paper documents in binders	Personal data erased after seven years (+ current year)	Accounts staff
Email	Email system	• In general, all email which is not needed for work is erased • Email in the deleted items folder and the "sent" folder should be cleaned out every third month • Other saved/archived email must be reviewed and cleaned out at least once a year. At the same time, own address book and own distribution lists should be cleaned out.	Everyone with an email account is responsible for their own email
Email, shared address book	Email system	Kept up to date on an ongoing basis	IT administrator

ERASURE ROUTINES FOR PERSONAL DATA ABOUT EMPLOYEES

These routines apply first and foremost to employees with personnel responsibility, for employees in IT administration, HR and payroll administration as well as others who process personal data about employees in their work.

In conjunction with recruitment/before employment:

- Unsolicited applications which are uninteresting must be erased immediately by the person receiving the application.

- Application documents that are part of a recruitment process must be erased two years and two months after recruitment is completed (i.e. when the statutory period for bringing an action for discrimination has expired). After recruitment is completed, application documents are only saved by the recruiting manager and/or HR. The manager/HR is responsible for erasing the documents.

- In order to save application documents for possible future recruitment consent is required. Application documents that are saved following consent must be erased after two years (or when consent is revoked). The person saving the application must ensure that consent has been given and that the documents and consent are erased after two years.

- Application documents for a person who is then employed must be saved throughout the period of employment. They are saved by the immediate manager and possibly also by HR.

During the employment period:

- When an employee changes manager during employment, e.g. at a reorganisation, the original manager must hand over all relevant personal data to the new manager in conjunction with the change of manager. The original manager must then erase the employee's personal data that he/she holds.

- Holiday lists must be erased by the person who created the list no later than three years after the end of the holiday year to which the list applies.

- Lists of conference participants and similar must be erased when they are no longer relevant, but after three years at the latest. Information on dietary requirements must always be erased as soon as the conference is over. Erasure must be done by the person/function that arranged the conference. Note that some bookkeeping details may need to be saved for a longer period (see below).

- Minutes under the Co-determination in the Workplace Act (MBL) must normally be erased by the person saving the document five years after negotiations have been completed.

- Lists of participants in training courses must be erased when they are no longer relevant, but after ten years at the latest. Information on dietary requirements must always be erased as soon as the course is over. Erasure must be done by the person/function that arranged the course.

- The result and personnel lists from employee surveys must be erased after 10 years. Erasure is done by HR and possibly others who have saved this information.

- Lists from salary reviews must be erased after 10 years. Erasure is done by managers, HR and others who have saved this information.

- Notes from performance development reviews (PDR), from labour law measures (such as reminders, warnings, reassignments) and from rehabilitation must be erased when they are no longer relevant but at the latest after 10 years. HR and the immediate manager are responsible.

- Information on occupational injuries or incidents must be erased 10 years after the event. HR and the immediate manager are responsible.

- Personal data (name and age) of an employee's children must be erased when the child has reached age 14 but at the latest two years after termination of employment. This is done by the payroll coordinator.

- In the event that the payroll coordinator receives information on an employee's health/diagnosis, e.g. from a doctor's certificate that is sent in, this information must be erased immediately. Other information in the doctor's certificate can be saved for as long as it is relevant.

Before termination of employment:

- The employee who is leaving must be required to erase all private documents from his/her area on the company's server, his/her work computer, his/her email as well as physical documents. In the event that an employee has used a mobile phone and tablet belonging to the company in his/her work, a corresponding erasure must be made on these devices. This must be done on the last day of employment at the latest.

- Documents, lists and email containing personal data which have been processed on behalf of the company *and which the company still needs* must be handed over in a structured manner to the successor or the immediate manager. Other documents with personal data must be erased. This must be done on the last day of employment at the latest. The immediate manager is responsible for ensuring that this is done.

- The employee's email address can if required remain active during a transition period of *maximum 6 months* with the aim of allowing the person(s) taking over the employee's duties to monitor messages during that period. The email address and associated mailbox is then deleted by the IT administrator.

When employment has terminated:

In conjunction with termination of employment (at the latest 1 month after termination unless otherwise stated)

- The employee's login account for the IT environment is deactivated as soon as possible by the IT administrator.
- Information in the login account that is no longer necessary (e.g. telephone number, company address and title) is erased as soon as possible by the IT administrator.
- Name, photos and other personal data must be removed from the public website, intranet, organisation chart, etc. The immediate manager is responsible.
- Documentation from performance development reviews (PDR) as well as all other documents with personal data which cease to be relevant since employment has terminated must be erased by the immediate manager, HR and payroll coordinator.
- Accounts/HR/payroll coordinator must inform company health care, insurance company, Rikskortet and other benefit partners that the person has left and that his/her personal data should be erased by them as completely as possible.
- Personal data in the facility entry system, including lists for receipt of keys and entry cards, are erased as soon as possible after termination of employment (and keys, etc., have been returned). This is done by the IT administrator or someone else with access to the system.

At the latest three months after termination of employment

- Bank account number is erased by the payroll coordinator as soon as final salary has been paid.
- Contact details of next of kin must be erased as soon as possible by the payroll coordinator.
- Address details, telephone number, details of children, citizenship, registration number of company car, etc., are erased by the payroll coordinator three months after termination of employment. (Note that details associated with length of service, salary payments and other remuneration, reason for termination for example must be saved for a longer period.)

At the latest six months after termination of employment

- Email account and Windows AD account are erased by the IT administrator.

Two years after termination of employment

- Application documents, reminders and rehabilitation documentation, etc., must be erased two years after termination of employment. Erasure is done by the manager/HR/the person who saved these details.

Seven years (+ the current year) after termination of employment

- Personal data in bookkeeping information such as vouchers, contracts and other documents must be erased. Erasure is done by the payroll coordinator, accounts staff as well as anyone else who has saved this information.

Ten years after employment has terminated

- Details in the payroll system that are associated with salary payments must be erased 10 years after termination of employment. Note however that details that are required to calculate pension provisions must be saved for a longer period (see below). The payroll coordinator is responsible for erasing this information.

When an ex-employee reaches 68 years of age

- At this time (10 years after normal pension age) all remaining personal details are erased, i.e. the entire contract of employment and other details that have been used to calculate pension provisions. The payroll coordinator and accounts staff are responsible for this erasure.

Summary of erasure routines for personal data about employees

BEFORE EMPLOYMENT

Document type/subject	Storage place	Erasure routine	Responsible	Other
Unsolicited applications that are uninteresting	In the email system (possibly on paper)	Erased immediately after the applicant has received a reply	The person receiving the application	
Application documents that are part of a recruitment process	In an own folder on the company's server and in the email system (possibly on paper)	Erased two years and two months after recruitment is completed	The person saving the application	
Application documents saved for possible future recruitment	In an own folder on the company's server	Erased after two years or when consent is revoked	The person saving the application	Consent required!

DURING EMPLOYMENT

Document type/subject	Storage place	Erasure routine	Responsible	Other
Change of manager – the employee gets a new manager	In an own folder on the company's server	The original manager must hand over all relevant personal data to the new manager and then erase all information that is not relevant	The original manager	
Trade union negotiations/protocol under the Co-determination in the Workplace Act (MBL)	In an own folder on the company's server	MBL protocol must be erased at the latest five years after negotiations have been completed	The person saving the document	
Holiday lists	In a common folder on the company's server	Erased at the latest three years after the end of the year to which the list applies	The person who created the list	
Conferences/company events – lists of participants Conferences/company events – dietary requirements	In an own folder on the company's server	Erased at the latest after three years Erased as soon as the conference is over	The person/ function that arranged the conference	
Training courses – lists of participants Training courses – dietary requirements	In an own folder on the company's server	Erased when no longer relevant, but at the latest after 10 years Erased as soon as the course is over	The person/ function that arranged the course	

Employee surveys	In an own folder on the company's server	Participant lists and results are erased after 10 years	HR and others who have saved this information	
Salary reviews	In an own folder on the company's server	Personal data must be erased after 10 years	HR and others who have saved this information	
Performance development reviews (PDR)	In an own folder on the company's server	Notes are erased when they are no longer relevant but at the latest 10 years after the review	Manager and others who have saved this information	
Rehabilitation	In an own folder on the company's server	Notes from rehabilitation are erased when they are no longer relevant but at the latest after 10 years	Manager, HR and any others who have saved this information	
Occupational injuries	In an own folder on the company's server	Information on occupational injuries must be erased 10 years after the event	Manager, HR and any others who have saved this information	
Details of children	Payroll system	All information on an employee's children must be erased when the child has reached age 14 but at the latest two years after termination of employment	Payroll coordinator	
Information on health/diagnosis	Payroll system	This information must be erased from a doctor's certificate or similar as soon as possible (other information in the doctor's certificate is saved for as long as it is relevant)	Payroll coordinator	

BEFORE TERMINATION OF EMPLOYMENT				
Document type/subject	**Storage place**	**Erasure routine**	**Responsible**	**Other**
Private documents and email	The company's server, the employee's work computer, email (also mobile phone and tablet if these are owned by the company)	The employee who is leaving must be required to erase all private documents saved on or through the company's IT resources as well as his/her private physical (paper) documents. This must be done on the last day of employment at the latest.	The employee who is leaving	The immediate manager is responsible for ensuring this is done
Work-related documents and email containing personal data	As above	Documents and email containing personal data which the company still needs must be handed over in a structured manner to the successor or immediate manager. Other documents with personal data must be erased. This must be done on the last day of employment at the latest.	The employee who is leaving	The immediate manager is responsible for ensuring this is done
WHEN EMPLOYMENT HAS TERMINATED – INFORMATION THAT MUST BE ERASED AS SOON AS POSSIBLE				
Document type/subject	**Storage place**	**Erasure routine**	**Responsible**	**Other**
Login account to the company's IT system	Active Directory server (as well as some other login servers)	The employee's login account is deactivated and personal data in the login account is minimised as soon as possible but at the latest one month after termination of employment.	IT administrator	
Email	Email server	The employee's email address may if necessary remain active for a period of up to 6 months after the termination of employment. The email account and mailbox must then be erased.	IT administrator	Somebody to monitor the email mailbox must always be assigned. This is done by the immediate manager
Public website, intranet, organisation chart, etc.	Web servers (internal and external), company server	All personal data including photos are erased as soon as possible but at the latest one month after termination of employment.	Immediate manager	
Performance development reviews (PDR)	In an own folder on the company's server	Documentation is erased. Time as above	Immediate manager, HR	

External benefit partners such as company health care, insurance, Rikskortet, etc.		External benefit partners must be informed that the person has left and that his/her personal data should be erased by them as completely as possible. Time as above.	Accounts/Payroll coordinator /HR	
Name and codes in the entry system, receipts for keys, entry card, etc.	Entry system, in an own folder on the company's server, in a physical binder	Personal data is erased as soon as possible but at the latest one month after termination of employment	IT administrator or someone else with access to the system	Updated list must be sent to the security company
Contact details of next of kin	Payroll system	Erased as soon as possible not later than 3 months after the employment has ended.	Payroll coordinator	
Bank account number	Payroll system	Erased as soon as possible not later than 3 months after the employment has ended.	Payroll coordinator	
Address details, telephone number, details of children, citizenship, company car	Payroll system	Erased 3 months after the employment has ended	Payroll coordinator	Details associated with salary payments and other remuneration as well as information on duration of employment, are saved for a longer period
WHEN EMPLOYMENT HAS TERMINATED – INFORMATION THAT MUST BE SAVED FOR A LONGER PERIOD				
Document type/subject	**Storage place**	**Erasure routine**	**Responsible**	**Other**
Application documents, reminders, rehabilitation	In an own folder on the company's server	The documentation must be saved for two years after termination of employment and then erased	HR and immediate manager	
Information on actual attendance and reason for termination	Payroll system	Erased seven years (plus current year) after termination of employment	Payroll coordinator	Information is required for replying to inquiries from an unemployment fund or the Swedish Social Insurance Administration

Personal data in bookkeeping information	Business system as well as paper documents in binders	Personal data in bookkeeping information such as vouchers, contracts and other documents is erased seven years after the calendar year in which employment terminated	Payroll coordinator, Accounts	
Details associated with salary payments	Payroll system	Erased ten years after termination of employment	Payroll coordinator	
All remaining personal data including details used to calculate pension provisions	Payroll system, accounting documents, own folder on company's server	Erased when an ex-employee reaches 68 years of age (If more that 10 years has passed since the employment ended)	Payroll coordinator, Accounts, Manager/HR	