Privacy policy – Kredinor SA

Prepared by Kredinor SA

Kredinor SA, through its CEO, Tor Berntsen, is responsible for processing. The person responsible for treatment is responsible for Kredinor SA to fulfill obligations under the privacy legislation. Kredinor's privacy representative is Linn Hagesæther.

Date: 27. april 2021

Responsible for processing:
Kredinor SA ved CEO. Tor Berntsen,
Organization no. 953556472
Email: tor@kredinor.no
Phone: 22009206
Postal Address: Postboks 782 Sentrum, 0158 Oslo

Privacy representative
Linn Hagesæther
Email: personvernombud@kredinor.no
Phone: 55573305
Postal Address: Postboks 1874 Nordnes, 5817 Bergen

Contents

Privacy policy -Kredinor SA

1) About our privacy policy

This privacy policy contains information that you are entitled to receive when your personal data is collected and processed. In the following, “personal data” means any information relating to an identified or identifiable natural person (data subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. Please read this statement carefully as it contains important information about how Kredinor processes your personal data and what rights you have in that regard.

This policy statement explains what personal information is collected about you and for what purpose, how the information is collected and protected, to whom this data is disclosed, and what rights you have if your personal data is registered with us.

Security and confidentiality regarding the processing and storage of your personal data and your financial situation are fundamental to our business. Kredinor has a duty to comply with the rules set out in the EU’s General Data Protection Regulation (GDPR) and the Norwegian Personal Data Act with respect to securing personal data, safeguarding your rights, notification of infringements, etc.

Kredinor SA, represented by its CEO, is responsible for the processing of personal data that takes place in our business. In the course of our business, we collect and process personal information. Which personal information is processed and how it is processed depends on the individual’s relationship with Kredinor.

Kredinor processes personal information about individuals (debtors) who have a debt that is being collected by us. We also process personal information about individuals designated as points of contact at established and future clients and suppliers, as well as visitors to our website, www.kredinor.no. Personal information about individuals who are party to a case being handled by our legal department, Advokatfellesskapet Bratsberg, is also processed. The processing of personal data in these different relationships is subject to different rules. For this reason, they are described separately in this policy statement, see points 3 to 5 below.

Kredinor also processes personal information about clients’ own customers in our invoice and ledger administration (Invoicing services) and through the operation and administration of the payment solution Let’s pay. In this relationship, Kredinor is the data processor and processes the information according to instructions from the creditor who is the data controller. Detailed information about this type of processing may be obtained by contacting your creditor.

2) Which regulations govern Kredinor’s processing of personal data

Regulations governing Kredinor’s processing of personal data

Kredinor processes personal data about you within the framework of the rules set out in the EU's General Data Protection Regulation (GDPR) and the Norwegian Data Protection Act, the industry standard for the processing of personal data in the Norwegian debt collection industry, as well as other special legal rules on the processing of personal data. An overview of the most important regulations for Kredinor’s processing of personal data can be found below.

- The EU's General Data Protection Regulation (GDPR)
- The Data Protection Act (Personopplysningsloven, in English)
- The Industry standard for the processing of personal data in the Norwegian debt collection industry (In Norwegian)

3) How we process your personal data if you are a debtor/end customer

Relationship – individuals who have a debt being collected by Kredinor (debtor/end customer)

3.1.The purpose of the data processing

Kredinor collects and processes personal data about you when we initiate debt collection proceedings on behalf of a client. The purpose of Kredinor's claims handling and case processing is primarily to obtain payment or ensure claim protection and customer follow-up should legal action subsequently be required to recover the debt.

Personal data collected for the purpose mentioned above will also be processed in connection with internal control procedures, testing, troubleshooting and maintenance of Kredinor's operating and security systems. The purpose of this processing is to safeguard our statutory duty to meet the security requirements set by the GDPR and to comply with the requirements of the Norwegian ICT Regulations for complete, timely and correct processing as well as the retention of data.

Personal data collected in connection with the recovery of outstanding debts is also used for analytical purposes. Only statistical data deriving from such analyses is disclosed to our clients. Personal data is not disclosed in this regard.

3.2. What personal data is collected and how it is processed

When registering a debt collection claim, Kredinor receives basic information about you from the creditor, such as your name and contact details, as well as information about the claim we have been commissioned to collect on the creditor's behalf. If the creditor has information about your date of birth or national identity number, we will also receive this. This information is collected to ensure that the claim and all associated actions are addressed to the correct person.

Information about your name and address provided by the creditor is compared against available public sources and Kredinor's own database to ensure you have been correctly identified, as well as to verify, correct, supplement and store the information. We will search for your current address in the Norwegian National Population Register and the Electronic Address Update facility used by the postal service. Your phone number is collected from Bisnode. If your national identity number is not provided by the client, this will be collected from the Norwegian Tax Administration.

Kredinor also collects and processes additional personal data, including various categories of financial information, such as information about your income and assets, as well as credit history. Such information is collected from available public sources and credit rating agencies.

Kredinor also processes personal data received directly from you. This may be information about your life situation, professional status and marital status. In some cases, we will collect other personal data concerning your health or criminal record, for example. Kredinor also processes information about you that we receive from others, such as a bailiff, court of law, the Norwegian Labour and Welfare Administration (NAV), a guardian/conservator, lawyer, debt counsellor, doctor, family member, employer, bank or others who contact Kredinor in connection with your case. Submitting personal information to Kredinor is voluntary.

Pursuant to the data protection regulations, only personal data that is relevant and necessary for a specific purpose may be collected. Kredinor processes only personal data that is necessary for the purpose of payment follow-up and debt

collection. The basis for which Kredinor collects and processes your personal data are therefore lawful. Personal data is not processed in a manner that is incompatible with these purposes.

3.3 Legal basis for data processing

The processing of personal data is only lawful when it has a legal basis.

Kredinor's legal entitlement to process personal data in connection with the collection of outstanding claims on behalf of our clients is covered by Article 6(1)(c) of the GDPR, which states that processing must be necessary for the fulfilment of a legal obligation, see Article 6(3)(b). The processing of personal data for this purpose is established in Norwegian law by virtue of the Debt Collection Act.

Thus, debt collection activities are carried out on the basis of an authorization/licence granted by the Financial Supervisory Authority of Norway. Furthermore, the regulations governing debt collection activities, established through circulars from the Ministry of Finance and the supervisory authority, include the processing of personal data such as the debtor's income, assets, debt, expenses, collateral, etc.

The legal basis for processing special categories of personal data is Article 6(1)(c) of the GDPR, see Article 6(3)(b), and Article 9(2)(e), which covers processing relating to personal data which has manifestly been made public by the data subject.

The legal basis for processing personal data about criminal convictions and violations of the law is Article 10 of the GDPR and Section 11 of the Personal Data Act, see Article 6(1)(c) and 6(3)(b).

The legal basis for processing personal data in connection with internal control procedures, testing, troubleshooting and maintenance of the operating and security systems comprising Kredinor's debt collection system is based on Article 6(1)(c) and 6(1)(f) of the GDPR, which provide that processing is lawful if it is necessary to fulfil a legal obligation or safeguard a legitimate interest that weighs heavier than the privacy of the individual.

Kredinor's interest in processing your personal data in such a context is rooted in our statutory duty to meet the security requirements set by the GDPR and the Norwegian ICT Regulations.

The legal basis for processing collected personal data for analytical purposes is the same as for Kredinor's legal entitlement to process your personal data in connection with the collection of debts on behalf of our clients, see above. Analytical material is limited to statistical data and does not contain personal data. Reference is made in this regard to Article 5(1)(b) of the GDPR.

In connection with debt collection proceedings, the processing of your personal data does not require your consent. However, should any subsequent processing be subject to your consent, you may withdraw this at any time.

3.4. Disclosure of personal data

Access to your personal data is limited primarily to employees of Kredinor in their professional capacity. All our employees have a statutory duty of confidentiality with respect to all matters concerning your case. Any communication with Kredinor SA is subject to the same duty of confidentiality.

We do not disclose personal data to others unless required to do so by law or regulation, disclosure is necessary to fulfil an agreement with the creditor, pursuant to Chapter 5 of the Debt Collection Act, or in connection with extra-judicial and/or legal proceedings. For example, disclosures may be made to judicial authorities, business partners, expert witnesses, employers, the Norwegian Labour and Welfare Service (NAV), social services, debt counsellors, the Norwegian National Population Register, the Norwegian postal service, the Brønnøysund Register Centre, The Norwegian Mapping and Cadastre Authority, yourself, the person appointed as your guardian/conservator or the person you have authorized to represent you. Personal data may also be disclosed to others if this is necessary to protect your rights.

When carrying out payment transactions, the personal data necessary to complete the transaction will be disclosed to the recipient's bank, and its assistants where necessary.

If you are resident abroad and the matter is not resolved at Kredinor's request, the case will be sent to our business partner in the country where you live. Personal data necessary to collect the debt in that country will then be disclosed to our partner, who is an independent data controller. In the event that debt collection is sought through public authorities in another country, such as the naming authority or other judicial authority, the necessary personal data will be disclosed to them.

If the debt collection assignment is transferred to a partner located in a third country, necessary measures will be taken to ensure an adequate level of data protection. Reference is made to the section below concerning the transfer of personal data to third countries.

Like other debt collection agencies, Kredinor uses a variety of subcontractors to enable it to provide its services. Our subcontractors are subject to the same obligations with respect to the security of personal data as Kredinor.

3.5. Decisions based on automated processes – scoring

Kredinor actively uses its own database and credit information to select the appropriate method of securing payment in each case, i.e. we score the case. The score tells us something about the likelihood of a debt collection case being resolved within a given time frame. To arrive at the score, Kredinor uses variables connected to the debtor's ability and willingness to pay.

The score predicts the probability of resolving the individual case on the basis of the total debt collection history across all Kredinor's clients in the past 12 months. The score can be anywhere along a scale from 0–100 per cent, with the choice of payment follow-up method depending on the final score.

The following main variables are included in debt collection scores:
• The size of the claim
• Average age of received claims
• Income and assets from the debtor's tax assessment
• Information about income and assets from the equation
• Average collection time for all claims
• The debtor's share of resolved, unresolved and active claims

The score has no legal effect or impact on you, as it is used to plan and take more precise actions during the follow-up of the claim until payment is received.

3.6. Storage restrictions (deletion)

Personal data is processed only for as long as is necessary to carry out the specific purpose for which it was collected.

Kredinor follows the rules covering restrictions on the storage of personal data set out in Article 5(1)(e) of the GDPR and the relevant rules in the industry standard for the processing of personal data in the debt collection industry, which has been prepared by the debt collection agencies in cooperation with the Norwegian Data Protection Authority. Pursuant to section 7.7, personal data in a debt collection case is deleted three years after the claim has been paid and the case resolved. Personal data in debt collection cases that have not been paid is deleted one year after the claim's time limit has expired. Personal data relating to claims misdirected by Kredinor or revoked by the client is deleted one year after the case is closed. Kredinor has a system solution which ensures automatic anonymization of personal data related to debt collection cases when the industry standard's mandatory deletion deadline expires.

4) How we process personal data about those designated as contacts for creditors/clients/suppliers

Relationship: points of contact with our clients and suppliers

Kredinor collects and processes personal data about you, if you have been designated as a point of contact by a member, client or supplier, as well as a potential client.

4.1. The purpose of the data processing

Data is processed for the purpose of entering into and managing our contractual relations with the organization you represent. We also process personal data about you for the purpose of organizing courses, conferences or other events arranged by Kredinor which you attend, or to enable you to receive newsletters from Kredinor.

The purpose of collecting and processing personal data about you in your capacity as a point of contact at a potential client is to market our services and engage in other sales-related initiatives.

4.2. What personal data is collected and how it is processed

When an agreement is entered into with Kredinor, personal data such as your name, e-mail address, phone number, employer and, potentially your job title, are collected and processed to obtain necessary contact details. This information is collected directly from you or from the entity you represent.

Similar information about points of contact with potential clients is obtained from public sources, such as the Brønnøysund Register Centre, the organization's website, gulesider.no. When Kredinor is invited to take part in a tender competition, such personal data is disclosed by the entity requesting the service or deliverable concerned.

4.3. Legal basis for data processing

Kredinor's lawful entitlement to process your personal data as a representative of a member, client or supplier derives primarily from Article 6(1)(b) of the GDPR, which specifies that such processing must be necessary to fulfil an agreement to which the data subject is party, or because such processing is necessary to fulfil a legal obligation that the data controller has incurred; see also Article 6(1)(c) of the GDPR.

Processing may also be necessary on the grounds of a legitimate interest, see Article 6(1)(f) of the GDPR. Kredinor's clients can consent to receive newsletters and invitations to courses, seminars or other events. Consent constitutes grounds for the processing of personal data necessary to distribute such information, see Article 6(1)(a) of the GDPR. Where consent constitutes grounds for processing, you may withdraw your consent at any time.

Kredinor's legitimate interest in being able to market itself and take steps to sell its services constitutes grounds for the processing of personal data relating to points of contract at potential customers, see Article 6(1)(f) of the GDPR.

If you do not wish your personal data to be registered with Kredinor, you may ask to have it deleted.

4.4. Suppliers

Kredinor uses a variety of subcontractors to enable it to provide its services. Our subcontractors are subject to the same obligations with respect to the security of personal data as Kredinor.

Kredinor has entered into data processing agreements with subcontractors, and is entitled to perform security audits to ensure that the subcontractor is processing personal data in compliance with the data processing agreement and prevailing data privacy regulations.

4.5. Automated decisions

We do not use automated decision-making processes when processing personal data about representatives of clients and suppliers.

4.6. Storage restrictions (deletion)

Personal data about points of contact at clients or suppliers is deleted five years after the business relationship ends, unless there are grounds for processing the data for a longer period.

Personal data about points of contact at potential clients is deleted no more than one year after it was recorded, unless the data subject consents to storage for a longer period. If a formal customer relationship is established, the data will be deleted five years after the customer relationship has ended.

5) How we process the personal data of those who use our legal services

Relationship: A party to a case being handled by the law firm Advokatfellesskapet Bratsberg.

Kredinor SA's legal department, the law firm Advokatfellesskapet Bratsberg, provides various legal services. When providing legal services to our clients, we are deemed the data controller.

5.1. The purpose of the data processing

Personal data is processed by our legal department for the purpose of establishing and managing a customer relationship, case management, collecting information about the opposing party and third parties, billing of legal fees and knowledge management.

5.2. What personal data is collected and how it is processed

The nature of the information collected and processed varies according to the type of case. We collect only such information as is relevant and necessary to provide the required assistance. When initiating a case, we obtain information concerning your name, address, phone number and e-mail address, as well as other data needed to perform our services. As the case proceeds, further personal data may emerge through case-related queries, correspondence and meetings. In some cases, other categories of personal data may be processed.

We process personal data about our clients, the opposing party in a client's case and any third parties. Personal data is obtained primarily from our clients. In addition, we receive personal data from the opposing side, their legal representatives, judicial bodies or other third parties, through queries and correspondence relating to the case.

5.3. Legal basis for data processing

Our legal department processes personal data primarily in connection with fulfilment of an agreement with a client. For client management and billing, the legal basis for processing will be Article 6(1)(b) of the GDPR, which specifies that processing is lawful if it is necessary for the fulfilment of an agreement to which the data subject is a party. For business customers, the legal basis for client administration will rest on a legitimate interest, see Article 6(1)(f) of the GDPR.

Lawful grounds for the processing of personal data in ongoing legal proceedings and for our knowledge management activities will be Article 6(1)(f), and will rest on the fact that such processing is necessary for purposes relating to the legitimate interests that are being pursued by the law firm, if such interests are not overridden by the fundamental rights and freedoms of the data subject.

Pursuant to Article 9(2)(f) of the GDPR, certain categories of personal data may be processed in connection with actions to determine, assert or defend a legal claim. The processing of data concerning legal judgments and offences will, in this context, be permissible pursuant to Article 10, see Article 11, of the GDPR.

In many circumstances, the law firm is subject to legal obligations that necessitate the processing of personal data, see Article 6(1)(c) of the GDPR. Examples of this include the processing of accounting material, any transactions presuming verification of the client's identity under the Norwegian Money Laundering Act, and the monitoring/follow-up of security incidents relating to our computer systems.

If no other legal grounds exist, or it is uncertain whether other grounds are sufficient for the processing of data, processing pursuant to Article 6(1)(a) will be based on the consent of the data subject.

5.4. Disclosure of personal data by the law firm

The law firm Advokatfellesskapet Bratsberg will not disclose your personal data unless there are legal grounds therefor. Such grounds will typically be an agreement with you or a statutory provision that compels us to disclose the information.

In conjunction with a commission to provide legal services, relevant personal data may typically be disclosed to the opposing side and judicial bodies in the form of correspondence and legal filings, in meetings between the parties and in judicial hearings.

Lawyers are subject to a strict duty of confidentiality with respect to privileged disclosures from the client. They are also obligated to keep information confidential, pursuant to the rules governing good legal practice.

Personal data that is processed by the law firm will also be accessible to the system supplier and the IT operations supplier which, in their capacity as data processors, provide services to Kredinor.

5.5. Automated decisions

We do not use automated decision-making processes to process personal data about parties to cases being handled by the law firm.

5.6. Storage restrictions (deletion)

Personal data in our client archives is stored for ten years to ensure documentation of how the case has been handled, in the event of any dispute involving or against the law firm.

6) What digital footprints do you leave behind when you visit Kredinor.no?

6.1. Cookies

When using the internet, you leave behind digital footprints which enable others to follow your online activities. Kredinor collects this type of data for the purpose of statistical analysis. We are not interested in your personal online usage, and therefore use this information only as statistics to improve our services. Your personal internet use is covered by a duty of confidentiality and is anonymized.

When you visit Kredinor's website, the following data is recorded:

- Which pages at kredinor.no you visit
- Which web browser you are using
- What screen resolution you are using

- Which operating system you are using
- Which link you used to arrive at our website
- Your IP address
- Which version of Java you are using

To obtain this information, Kredinor makes us of so-called “cookies”. A cookie is a small text file that is placed in your web browser’s internal memory when you visit kredinor.no. Information about our use of cookies is published on the website kredinor.no. The use of cookies requires your consent. If your web browser is set up to automatically accept cookies, this meets the requirements for consent. However, if you do not wish to accept the use of cookies, you can change the settings in your web browser. There, you can also delete any cookies that have already been installed.

The website kredinor.no uses cookies to create a more user-friendly experience by identifying where the visitor has come from and how they use the site once they have arrived. In some cases, we use IP addresses to log navigation at kredinor.no. None of the cookies can link information about the use of kredinor.no to the user as an individual. Data derived from kredinor.no is processed by Kredinor’s marketing department, IT department and those suppliers used for maintenance, development and advertising (only companies, not private individuals) and searches on the website.

Information on how to delete cookies (in Norwegian – try a search for other language).

6.2. Digital footprints when you visit “My Page”

On the login page, My Page, cookies are used when logging in and to obtain correct data about the logged-in user. My Page requires the user to permit cookies to enable them to access their own information and use services such as making payments and applying for an instalment arrangement. The date of your visits to the My Page facility is also logged. If you communicated with Kredinor via My Page, what you write will be stored until the case is anonymized.

6.3. Analysis

Kredinor uses the analysis tools Google Analytics and Siteimprove Analytics to map use of kredinor.no by means of the types of cookies indicated in the table below.

Kredinor uses the IP anonymization function in Analytics and Siteimprove. Complete IP addresses are not recorded.

Name of cookie	Function/purpose	Analysis tool/supplier
siteimproves	Collects data on which pages the user visits on the website.	Siteimprove Analytics
nmstat	Tracks the user’s visits to the website, e.g. statistics on the user's most recent visit to the site.	Siteimprove Analytics
szcookiechoice	Is used to determine whether the user has accepted the use of cookies or turned them off.	Siteimprove
__utmz	Identifies where the user comes from when clicking onto kredinor.no (search engine, keyword, link, advert, etc).	Google Analytics
__utma	Notes how many times the user has visited kredinor.no, to determine the number of first-time users and return visitors.	Google Analytics
__utmb / __utmc	Tracks the time spent by the user at kredinor.no.	Google Analytics
PHPSESSID	Stores information about a session – one single visit.	PHP
vlmref / vaid	Collects data on a unique user session and reports how many unique visitors and sessions we see from various companies, and what pages they look at (not down to the individual person).	Vendemore

6.4. Forms – kredinor.no

Contact details that are voluntarily provided in forms on kredinor.no are used only to follow up the query. This information is not stored in any cookies.

5. Processing of personal data in chats

On Kredinor's website, it is possible to put questions to our chat robot Nora. Any personal data entered as part of the chat is processed by Kredinor. The service is access controlled, and access is restricted to people who are responsible for answering queries via the chat function, in addition to Kredinor's point of contact at Boost, which supplies the system used. An automatic delete function has also been installed in the software. This ensures that national identity numbers are immediately anonymized once a message has been written and sent. This means that the NID is not stored or visible in the chat log. The delete function works such that all number combinations containing 7 digits or more are automatically deleted.

7) Will personal data be transferred to a third country?

7.1. Transfer of personal data to a third country

A third country is any country outside the EU/EEA that has not been approved by the European Commission. The transfer of personal data to third countries must take place in compliance with Article 44 et. seq. of the GDPR.

Kredinor makes use of an IT operations supplier which, in addition to its head office in Norway, has an operations department in a third country. The relationship between the operations supplier and the third-country department is regulated in an EU-approved standard contract, see Article 46(5) of the GDPR.

For the development of Kredinor's IT solutions, Kredinor uses a supplier with a development team in a third country. The relationship between the supplier and the third-country development department is regulated by binding business rules, see Article 46(2)(b) of the GDPR.

Contact Kredinor for further information concerning the implementation of safeguarding measures.

8) What rights do those registered with us have?

Anyone is entitled to request basic information about the processing of personal data at Kredinor. This privacy policy contains such basic information.

8.1. Right to access

If you are registered in one of Kredinor's systems, you are entitled to obtain information about the personal data concerning you we process when Kredinor is the data controller.

With those restrictions following from the GDPR, your right of access to information encompasses the purpose for which we process your personal data, which data we process, who we obtain your personal data from, who we disclose your personal data to, how long we store your personal data, whether your personal data is included in automatic decision-making processes, how we protect your personal data, and what rights you have. This privacy policy addresses several of these issues.

If you are the subject of a debt collection claim that we are handling on behalf of a client, you may log in to My Page at kredinor.no/mypage. Here, you can download an access report where you will find information about the personal data

concerning you that Kredinor processes. Select “Personal and credit data” in the menu, and then select “Archive”. You will have to log in to My Page using BankID (also BankID for mobile devices). If you do not have BankID, please contact our data protection officer to request access to your personal data. You will find contact details for the data protection officer at the end of this privacy policy.

If your personal data is being processed in connection with one of the other relationships with Kredinor specified above, please contact our data protection officer to gain access to your personal data.

Requests for access to personal data we process in our capacity as data processer should be addressed to the data controller. If Kredinor receives a request for access to personal data that we process at the instructions of a data controller, the request will be forwarded to the data controller, who will respond to your query.

8.2. Right to rectification and restriction

You have the right to request that personal data be rectified if it is incomplete or incorrect.

8.3. Right to restricted data processing

If you contest the accuracy of the personal data that Kredinor processes, if you believe the processing to be unlawful or you consider that the processing is no longer necessary to fulfil the purpose for which it was collected, you are entitled to request that its processing be restricted. The same applies if you have any objections to the processing of your personal data.

8.4. Right to erasure

You are also entitled to request that your personal data be erased. The right to erasure does not apply if Kredinor needs the data to fulfil the purpose for which it was collected or because its processing is necessary to fulfil a legal obligation or to determine, assert or defend a legal claim.

8.5. Right to withdraw consent

If the processing of personal data is based on your consent, you may withdraw your consent at any time.

8.6. Right to object to processing

You are entitled to object to Kredinor’s processing of your personal data, unless that processing is necessary to enable Kredinor to safeguard a legitimate interest, which weighs heavier than your privacy.

8.7. Right to complain

If you believe that Kredinor has not upheld your rights with respect to the Norwegian Data Protection Act, you are entitled to complain to the appropriate supervisory authority. Send your complaint to the Norwegian Data Protection Authority. You will find contact details for the Norwegian Data Protection Authority at www.datatilsynet.no.

9) Data security

About data security

Security and confidentiality concerning the processing and storage of your personal data and financial situation are fundamental to our business activities. In addition to our privacy policy and practice, we use a number of security mechanisms to protect your personal data and cases concerning you from unauthorized or unlawful processing and from inadvertent loss, damage or destruction. Some of our security measures are listed below:

- All employees, temporary staff, consultants and suppliers must sign a non-disclosure agreement before they are granted access to our professional systems and our premises.
- All employees, temporary staff and suppliers with access to personal data in our professional systems have a duty to familiarize themselves with our security policy. The security policy is reproduced in a security handbook, which the above-mentioned groups must read before they are granted access to the systems. Our security policy and security handbook are revised annually, and everyone has a duty to read and understand the revised edition.
- Kredinor provides internal user training with a focus on privacy and data protection.
- Kredinor has access control systems and safeguards sensitive personal data in a dedicated, secure zone.
- Technical security measures have been implemented to prevent hacking and illegal access to personal data.
- Kredinor has established technical solutions to encrypt personal data which our clients send to Kredinor and/or we send or disclose to our clients.

Please contact Kredinor for further details about our security measures.

10) Revision of the privacy policy

Revision

Changes to our services, rule changes, etc, could lead to changes in this privacy policy. The latest revision is dated 27 June 2018.

11) How to contact us if you have questions concerning personal data

Data protection officer:

Kredinor SA collaborates with the Norwegian Data Protection Authority through a dedicated data protection officer. The data protection officer is Kredinor's point of contact with the authorities and helps Kredinor to comply with the Data Protection Act.

Data protection officer:

Linn Hagesæther
E-mail: personvernombud@kredinor.no
Phone: +47 55573305
Postal address: PO Box 1874 Nordnes, NO-5817 Bergen, Norway

The data controller at Kredinor is the company's CEO Tor Berntsen. The controller is responsible for ensuring that Kredinor SA fulfils its obligations under the Data Protection Act.

Data controller:
Kredinor SA, in the person of CEO Tor Berntsen
Org.no. 953556472
E-mail: tor.berntsen@kredinor.no
Phone: +47 22009206
Postal address: PO Box 782 Sentrum, NO-0158 Oslo, Norway