
CLARKSONS
PRIVACY POLICY
CLARKSONS SECURITIES AS

TABLE OF CONTENTS

PRIVACY POLICY

1. Privacy statement

1.1. Introduction

The General Data Protection Regulation ("**GDPR**") and the Norwegian Personal Data Act regulate the use of private information in relation to Clarksons Securities AS' ("**CS**" or "**we**") business, employees, clients and relevant third parties. CS is responsible for your personal data as Data Controller according to applicable data protection legislation (including but not limited to GDPR.

This Privacy Statement ("Statement") sets out the policy statement for **CS** and will be supported by internal **p**olicies outlining further details on implemented measures and internal procedures.

The Statement applies to the personal data of our current, former and prospective clients, users of

our web site, visitors to our office, suppliers, collaborating partners and other people with whom we may interact. By using the services of CS, you consent to us processing personal data in accordance with this privacy policy and in compliance with the legislation applicable at any given time.

1.2. Controller and data processor

CS is the controller for the personal data processing unless otherwise stated. Controller means in this context a company, which alone or jointly with others, determines the purposes and means of the processing of personal data. Data processor means in this context a company which processes personal data on behalf of a controller.

CS is a regulated investment firm under the supervision of Finanstilsynet (The Financial Supervisory Authority of Norway). CS is subject to extensive record keeping requirements under the securities legislation and the anti-money laundering legislation.

The ultimate responsibility sits with the Chief Executive Officer. Daily follow-up is handled by Compliance.

2. How do we collect data?

2.1. Directly

CS obtain personal data directly from individuals in a variety of ways, primarily when clients are onboarded and use our services, but also when you provide us with a business card, subscribe to our newsletters/reports, request marketing to be sent to you, attend meetings or events we host, apply for a job, visit our offices, provide us with feedback or contact us.

Additionally, through the use of cookies and similar technologies, we may automatically collect Technical Data about your equipment, browsing activity and patterns.

2.2. Data collected from third parties

We obtain personal data indirectly about individuals from a variety of sources, both public and non-public.

Public sources - Personal data may be obtained from public sources, such as registers (companies registries shareholder registries etc.), news articles, sanctions lists, recruitment services, business intelligence services, social and professional networking sites, and internet searches.

Non-public sources – Personal data may also be obtained from non- public sources, such as credit rating agencies.

3. What categories of personal data do we collect?

3.1. Personal data

Here is a list of personal data we commonly collect to conduct our business activities.

- Contact details (e.g. name, company name, job title, marital status, gender, work and mobile telephone numbers, billing address, delivery address, email address both professional and personal email and postal address).
- Professional details (e.g. job and career history, educational background and professional memberships).
- Financial information (e.g. taxes, payroll, pensions, bank details, payment card details, insolvency records).
- Transaction Data (e.g. details about payments to and from you and other details of products and services you have purchased from us).
- Technical Data (e.g. internet protocol (IP) address, your login data, browser type and version, time zone setting and location, browser plug-in types and versions, operating system and platform and other technology on the devices you use to access this website).
- Profile Data (e.g. your username and password, purchases or orders made by you, your interests, preferences, feedback and survey responses).
- Usage Data (e.g. information about how you use our website, products and services).
- Marketing and Communications Data (e.g. your preferences in receiving marketing from us and your communication preferences).
- CCTV at our sites may collect images of visitors. Door logs and visitor passes may collect images and personal data such as name and email address.
- Photographs (e.g. at corporate events).

3.2. Sensitive personal data

We typically do not collect sensitive or special categories of personal data about individuals. When we do need to process sensitive personal data, it is with the consent of the individual unless it is obtained indirectly for legitimate purposes. Examples of sensitive personal data we may obtain include:

- Dietary restrictions or access requirements when registering for in-person events that reveal religious beliefs or physical health.
- Personal identification documents that may reveal race or ethnic origin, and possibly biometric data of private individuals, beneficial owners of corporate entities,
- or applicants.
- Adverse information about potential or existing clients and applicants that may reveal criminal convictions or offences information.
- Information provided to us by our clients in the course of a professional engagement.
- Diversity and equal opportunity information volunteered by applicants.

3.3. Child data

Although we do not intentionally collect information from individuals under 13 years of age, we may occasionally receive details about children, such as if they are a beneficial owner in a company which is a client with us.

3.4. Location-based data

We may process geographical locations you enter when seeking an office near you.

We also collect, use and share non-personal information such as statistical data for any purpose. This non-personal information may be derived from your personal data but is not considered personal data by the law as this data does not directly or indirectly reveal your identity. For example, we may aggregate your usage data to calculate the percentage of users accessing a specific website feature.

If we combine any non-personal information with your personal data so that you can be identified from it, we will treat the combined data as personal data which will be used and protected in accordance with this Statement.

4. What lawful reasons do we have for processing personal data and why do we need it?

We will use your personal data only where we have a lawful basis for doing so. We process your personal data for a number of purposes. The lawful basis for processing your personal data will depend on the purpose for which it was obtained. The table below sets out the purposes for which we may process your personal data and the relevant lawful basis/bases that allow for that processing:

The processing covers data relating to individuals, for corporate clients, we collect data that can be linked to individuals, such as client representatives, point of contact or beneficial owners.

Purpose of Processing	Type(s) of Data	Our Lawful Basis for Processing
Client on-boarding	> Identity Data > Contact Data > Social security number or corresponding tax identification number (TIN) > Bank account and, if applicable securities account > Information on political exposure > Citizenship The data we collect in connection with the establishment of a client relationship will be entered into our Onboarding provider Verified AB and client register - ProBroker.	> To perform a contract with you > Necessary to comply with a legal obligation
Managing our client relationship with you and the provision of other services to you.	We use personal data in connection with electronic information and marketing of our products and services, to the extent permitted by applicable law. We uses telephone, e-mail, SMS and other digital channels of communication in our client marketing. Such marketing takes place in compliance with the legislation applicable at any given time. If you do not wish to receive such communications, you may decline such communications at any given time.	> To perform a contract with you
Assessment of appropriateness and suitability **The securities legislation has extensive record keeping requirements, such as assessment of suitability and appropriateness. This information is used to give investment advice tailored to the client's investment objectives. We use this**	> Investment objective > Wealth and income details > Knowledge and experience	> Necessary to comply with a legal obligation > To perform a contract with you

personal information to ensure you have sufficient knowledge and expertise to understand the risk inherent in our products.		
Client communication and trades **The securities legislation requires regulated firms to store client dialogue on tampering-proof means of storage in order to retrospectively document how the parties have communicated with each other.**	CS record and keep all incoming and outgoing telephone calls made on a fixed line, mobile telephone and Teams by those of our employees engaged in client dialogue. We also keep e-mails and SMSs. CS also record all relevant information related to relevant face-to-face conversations with clients. The information we record include the following. • Date and time of meetings • Location of meetings • Identity of attendees • Initiator of the meetings • Face-to-face conversations that relate to the provision of client order services that relate to the transmission and execution of client orders, including such conversations and communications that are intended to result in transactions. We are, furthermore, required to keep documentation in respect of submitted orders and executed trades. This will document the behavioural patterns of individuals.	> Necessary to comply with a legal obligation
Compliance **Regulated firms are required to carry out comprehensive checks to ensure that their own business operations are conducted in compliance with applicable statutory requirements.**	This requirement means that we need to review stored dialogues with our clients, whether by e-mail, telephone, chat, etc. The dialogue with the client, potential client, supplier or business partner may be invoked as evidence in connection with proceedings	> Necessary to comply with a legal obligation

	before administrative appeal bodies or the courts of law. We will be able to identify relevant telephone communications by searches for incoming or outgoing telephone numbers, time of call and/or which employees participated in the call. We will be able to identify communications conducted via other communication channels on the basis of client identity, time of dialogue and which employees participated in the dialogue.	
Complaint handling and disputes **In the event of disputes between us and clients, potential clients, suppliers or business partners, it will be necessary for us to review stored client dialogue in order to determine the course of events.**	The dialogue with the client, potential client, supplier or business partner may be invoked as evidence in connection with proceedings before administrative appeal bodies or the courts of law.	> Nessecary for our legitimate interest*.
Reporting to the authorities **Complying with legal and regulatory obligations relating to countering money laundering, terrorist financing, fraud, market abuse, insider trading, sanctions evasion and other forms of financial crime.**	We are required to report any suspicious transactions to the authorities and will in such situations hand over related client details and client dialogues.	> Necessary to comply with a legal obligation
Requests from the authorities **The regulated entities within the group receives requests from financial regulatory authorities, tax authorities and the police/public prosecutors ordering us to disclose, pursuant to statute, client relationship documentation.**	We will in such contexts be required to disclose stored personal data in the form of client details and client dialogue.	> Necessary to comply with a legal obligation

*Legitimate interests means our legitimate interests in conducting and managing our business where these interests are not overridden by your fundamental rights, interests and freedoms.

5. What happens if you fail to provide personal data to us?

If you fail to provide personal data that we need to perform a contract with you or by law, then we may not be able to provide you with the product or service the contract relates to. We will notify you when this is the case.

6. Which personal data we collect in other relationships?

6.1. Potential clients

In order to find potential clients we use various publicly accessible sources, such as the shareholder registry (Aksjonærregisteret), proff.no, internet searches and news articles.

Marketing to potential clients are based on consent. Primarily we register consent through taped lines or incoming e-mails. Since the implementation of the GDPR consent are registered in a systematic manner in our CRM system SuperOffice. You can withdraw your consent at any time, by sending us and email or use the unsubscribe/Opt-out button.

For potential clients we collect the following data that can be linked to individuals:

Purpose of Processing	Type(s) of Data	Our Lawful Basis for Processing
Marketing	Contact details	> Consent
Communication **The securities legislation requires regulated firms to store client dialogue on tampering-proof means of storage in order to retrospectively document how the parties have communicated with each other. Also communication with potential clients will be stored on these tampering-proof means of storage.**	E-mail correspondence and telephone recordings.	> Necessary to comply with a legal obligation

6.2. Suppliers and business partners

For suppliers and business partners we collect the following data that can be linked to individuals:

Purpose of Processing	Type(s) of Data	Our Lawful Basis for Processing

We process personal data on suppliers and business partners to the extent necessary to manage and to fulfill an agreement and the ongoing business relationship.	Contact details	> GDPR Article 6 (1) (b) necessary for the performance of a contract to which the data subject is a party.
Communication **The securities legislation requires regulated firms to store client dialogue on tampering-proof means of storage in order to retrospectively document how the parties have communicated with each other. Also communication with suppliers and business partners will be stored on these tampering-proof means of storage.**	E-mail correspondence and telephone recordings.	> Necessary to comply with a legal obligation

6.3. Video recording by closed-circuit camera surveillance

We make video recordings by closed-circuit camera surveillance on our premises in order to prevent and detect any criminal activity. Such recordings are deleted on an ongoing basis after 7 days. On-site signs clearly indicate where recordings are made and who is responsible for such recordings.

7. Cookies and tracking

Our websites may use cookies. Where cookies are used, a statement will be sent to your browser explaining the use of cookies. To learn more, please refer to our cookie policy (https://www.clarksons.com/cookie-policy/).

We also use Singletrack for communication, sending research and marketing towards clients and prospective clients. We keep track of open rates, clicks, and segment data with a built-in analytics tool.

Click tracking allows us to see if contacts have clicked links to our research. Report will show which clients clicked our research links, and how many times each link was clicked.

When we use click tracking in a research report, Singletrack adds tracking information to each click-through URL. Each time a contact clicks a link in the campaign, the tracking information redirects them through Singletrack 's servers and sends them to the intended web address. That redirect through Singletrack' server is logged in our analytics tool as a click.

8. How long do we retain personal data?

We will not keep your personal data longer than is necessary for the purpose for which we use it. Unless a different time frame applies as a result of business need or specific legal, regulatory or contractual requirements, where we retain personal data in accordance with these uses. We will dispose of personal data in a secure manner when we no longer need it.

In some circumstances we may anonymise your personal data (so that it can no longer identify you) for research or statistical purposes in which case we may use this information indefinitely without further notice to you.

8.1. Clients

Statute	Type(s) of Data	Storage period
Securities Trading Legislations (e.g. MIFID)	Documentation and information required to be kept under the Securities Trading Legislations implemented from relevant EU directives, including client data and audio recordings.	Dependent on the information, the length of storage will vary from 5-10 years. All e-mail correspondence is retained for 10 years. All Bloomberg messages' and chat will be stored for 6 years. Tape recordings and SMS's are retained for 5 years.
Anti-Money Laundering Legislation	Documentation required to be kept under the Anti-Money Laundering Legislations , implemented from EU directives, including data relating to client checks	Minimum of 5 years after discontinuation of the client relationship or completion of the transaction
Bookkeeping Legislations	Accounting material	Accounting materials required to be kept 5 years after the end of the financial year. Accounting material must be kept for 10 year under certain circumstances such as after a merger or dissolution.

8.2. Potential Clients

Potential clients registered in our database under legitimate interest.

Personal data relating to potential clients will be deleted when the client withdraws its consent, CS may however store sufficient data on the potential client for up to five years, in order to avoid re-contacting the client within a reasonable timeframe.

8.3. Suppliers and business partners

Personal data relating to individuals with our suppliers and business partners, will be deleted at the latest ten years after the termination of the business relationship. Relevant information includes such as names, telephone numbers and email addresses. CS also collect bank details, so that we can pay you. We may also hold extra information that someone in your organisation has chosen to tell us. Our calls with you may be recorded and retained, depending on the applicable local laws and requirements.

8.4. People whose data we receive from staff and prospective members of staff, such as referees and emergency contacts

To ask for a reference for a prospective member of staff, CS need the referee's contact details (such as name, email address and telephone number). CS also need these details if our candidate or a member of our staff has put you down as their emergency contact so that we can contact you in the event of an accident or an emergency.

9. What about personal data security?

We have put appropriate technical and organizational security policies and procedures in place to protect personal data (including sensitive personal data) from loss, misuse, alteration or destruction. We aim to ensure that access to your personal data is limited only to those who need to access it. Those individuals who have access to the data are required to maintain the confidentiality of such information. We may apply pseudonymisation, de-identification and anonymisation techniques in efforts to further protect personal data.

If you have access to parts of our websites or other client log-inn or use our services, you remain responsible for keeping your user ID and password confidential. Please be aware that the transmission of data via the Internet is not completely secure. Whilst we do our best to try to protect the security of your personal data, we cannot ensure or guarantee the security of your data transmitted to our site; any transmission is at your own risk

10. Do we share personal data with third parties?

We may share personal data with trusted third parties to help us deliver efficient and quality services. These recipients are contractually bound to safeguard the data we entrust to them.

We may engage with several or all of the following categories of recipients:

- We disclose personal information to securities registers, shareholder registries, partner banks and other partners, including other companies in the Clarksons group (the " **Clarksons group (the "Group").**") structure, to the extent necessary to perform an agreement with you or provide services to you.

- When CS is entering into contracts with third parties, such as banks, we may be required to disclose personal data to that bank, in order for the bank to fulfil its own legal obligations.
- We will disclose personal information when we are legally obliged to do so, for example upon reporting of suspicious transactions or when disclosure is ordered by government authorities.
- Disclosure may also be necessary to comply with group-based management, control and/or reporting requirements laid down by statute, such as in the connection with the operation of the Group IT systems or disclosure is necessary to attend to the Group's interests in any dispute.
- The data subject consents to disclosure

CS conducts extensive business operations that rely on IT system operations procurement. The securities legislation makes such outsourcing subject to strict conditions. The service providers will either process personal data in the EU/EEA or in approved third countries with the same strict personal data legislation or subject to mechanisms that attend to data protection considerations in accordance with applicable regulations, for example the EU Standard Contractual Clauses or Privacy Shield certification (only in the US). Moreover, designated data processor agreements between CS and the IT service provider include comprehensive regulations on what information the service provider has access to, as well as how such information shall be processed in order to ensure compliance with CS' strict information processing procedures.

If CS transfers personal data abroad, it will do so in compliance with Norwegian law and the applicable mechanisms.

11. What are your data protection rights?

By law you have certain additional privacy rights. These are to:

> **be informed** of how we are processing your personal data – this privacy policy serves to explain this to you.

> have your personal **data corrected** if it is inaccurate or incomplete;

> have your **data erased (the right to be forgotten)** in certain circumstances – e.g. where it is no longer needed by us the purpose for which it was collected or you have withdrawn your consent. Please note however, that in certain circumstances, we may not be able to comply with your request of erasure for legal reasons. If this is the case, we will notify you at the time you request erasure;

> **restrict the use of** your data in certain circumstances e.g. where you have told us the data is inaccurate and we are in the process of checking this. In such circumstances we will continue to store your data but will not process it further until we have checked and confirmed whether the data is inaccurate;

> object to the processing of your data in certain circumstances - e.g. you may object to processing of your data for direct marketing purposes;

> **object to decisions being taken by automated means**; and

> to **withdraw your consent at any time** to processing where we are relying on consent as the lawful basis - e.g. to receiving marketing communications. Please note if you withdraw your consent, we may not be able to provide certain products and services to you - We will let you know if this is the case at the time you withdraw your consent.

> you have as well the right to **data portability** (transfer of your personal data to another controller), if this is technically feasible.

> you have the right to request access to any personal data we have stored in relation to you. All such requests must be sent to **compliance.oslo@clarksons.com**

You also have the right to file a complaint with the competent Data Protection Authority, which may be the supervisory authority in your country of residence or place of work if you believe that our personal data processing violates applicable legislation. The relevant authority for CS is the Norwegian Data Protection Authority https://www.datatilsynet.no/om-datatilsynet/kontakt-oss/

Please contact compliance.oslo@clarksons.com in the event you have further questions.