

NORDIC CLIMATE GROUP

Data Protection Policy

Table of contents

1.	Introduction.....	2
2.	Data protection concepts.....	2
3.	Principles for processing personal data.....	3
4.	Legal basis for processing personal data.....	4
5.	Data subject’s rights and information to data subjects.....	5
6.	Record of processing activities	6
7.	Data breach procedure	6
8.	Use of data processors and international data transfers	7
9.	Privacy by design and privacy by default	8
10.	Data protection impact assessments.....	8
11.	Personal data on social media platforms.....	8
12.	Use of cookies on websites and apps	9
13.	Implementation	9
14.	Reporting concerns and consequences of violation	9
15.	Review and follow-up.....	10

1. Introduction

When doing business, NCG Group AB collects, uses, and stores personal information about its employees, its customers, business partner representatives, and other individuals. NCG Group AB has a responsibility to ensure that it handles this information responsibly in order to protect their personal data.

This Data Protection Policy is designed to help NCG Group AB comply with the European General Data Protection Regulation (the “**GDPR**”). NCG Group AB also ensures to comply with supplemental or additional national data protection legislation applicable wherever NCG Group AB operates.

This Data Protection Policy applies to all employees and other contractors of NCG Group AB and its board of directors when they act in their capacity as directors of NCG Group AB.

2. Data protection concepts

<i>Controller</i>	When NCG Group AB processes personal data, it will usually do so on its own initiative, determining why and how the personal data will be processed, acting as “controller”.
<i>Data subject</i>	A data subject is an individual whose personal data is being processed
<i>Joint controllers</i>	Sometimes two or more organisations might work together to decide why and how personal data is processed. This is referred to as “joint controllership” and should be governed by a joint controller agreement that determines the controllers’ respective responsibilities.
<i>Personal data</i>	Personal data is information relating to an identified or identifiable individual, for example name, social security number, online screen name, location data, or an identifier such as their physical, physiological, genetic, mental, economic, cultural, or social identity
<i>Processing</i>	Processing is the handling of personal data, including collecting, using, adapting, transmitting, storing, and even erasing personal data.
<i>Processor</i>	“Processor” is the term given to companies processing personal data purely on behalf of, and under the instructions, of another company. When the Company engages third parties to provide it with services, these service providers usually act as processors (and the Company acts as the controller). Controller-processor relationships must be governed by a data processor agreement.
<i>Special categories of personal data</i>	Some categories of personal data are generally prohibited from processing, unless specific derogations apply. Such categories are sometimes referred to as ‘sensitive data’ and include personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

3. Principles for processing personal data

Certain principles apply to every data processing activity. NCG Group AB must comply with each of the principles described below.

<i>Lawfulness, fairness, transparency</i>	The Company must only process personal data on certain specific legal grounds, and must take into account any elevated risks to the privacy of data subjects. It must also ensure it is open and forthcoming with data subjects about what personal data of theirs it processes, and how the processing is performed.
<i>Data minimisation and purpose limitation</i>	Personal data may only be processed for specified, explicit, and legitimate purposes that are compatible with the original reason for collecting the personal data, and only to the extent necessary for achieving that purpose. NCG Group AB must not collect personal data on a “nice-to-have” basis. NCG Group AB’s systems and procedures should be designed to uphold these principles.
<i>Accuracy</i>	NCG Group AB must ensure that it takes active steps to ensure that the personal data it has on file is accurate and up-to-date.
<i>Storage limitation</i>	NCG Group AB must have a systematic approach to maintaining records in order to comply with applicable laws and regulations, to protect its interests, and for business continuity. Personal data, however, should not be stored for unnecessarily lengthy periods or without an overriding interest given the risk this poses to the privacy of individuals.
<i>Integrity and confidentiality</i>	NCG Group AB must implement appropriate technical and organisational measures to achieve an adequate level of security for its personal data processing activities. NCG Group AB must also ensure it maintains the integrity of its personal data processing activities, taking steps to prevent accidental data loss. In doing so, it will take into consideration relevant state-of-the-art technology; the costs of implementation; and the nature, scope, context, and purposes of the processing.
<i>Accountability</i>	The accountability principle requires NCG Group AB to take responsibility for and demonstrate compliance with processing personal data in compliance with the principles described above. NCG Group AB must have appropriate measures and document such measures, e.g. adopting and implementing data protection policies, maintain documentation of data processing activities, carrying out data protection impact assessments, etc.

What does this mean for me?

- Exercise particular care when collecting and processing special categories of personal data (i.e. sensitive personal data) and/or data relating to criminal convictions and offences.
- Respond in a timely manner to data subject requests (such as for information, access, or to be forgotten) in consultation with the Data Protection Compliance Officer.
- Keep personal data confidential, and implement a level of security appropriate to the risks presented by the processing, and nature, of the personal data.
- Report data breaches immediately, in accordance with NCG Group AB's procedure, given the strict time frame to do so under law.

4. Legal basis for processing personal data**4.1 Legal basis**

NCG Group AB can only process personal data if it identifies specific legal grounds permitting such processing. NCG Group AB should always be aware of which legal ground it is relying upon when carrying out a processing activity. More restrictive conditions apply to special categories of personal data, as explained below.

<i>Legal obligation</i>	NCG Group AB may process personal data to the extent necessary to fulfil a legal obligation (e.g. submitting tax income information to a national tax authority).
<i>Performance of a contract</i>	The data processing is necessary for NCG Group AB to fulfil its obligations in a contract that it has entered into with the data subject (e.g. retaining bank account details to pay a salary under an employment contract), or in order to take steps at the request of the data subject prior to entering into a contract.
<i>Legitimate interest of the Company</i>	NCG Group AB may process personal data for legitimate purposes as part of its business. (e.g. keeping a database of information on its customers or business partners, or collecting the names and phone numbers of emergency contacts of its employees). However, the legitimate interest must be specific, and justified when weighed up against the fundamental rights of the data subject, including their right to privacy.
<i>Consent</i>	The data subject has agreed to the processing (e.g. by signing up for a company newsletter). Consent must be freely given, specific, informed, and unambiguous. Data subjects must be informed that they can withdraw their consent at any time.
<i>Other</i>	Although they are rarely applicable, there are other grounds on which personal data may be processed, namely the protection of the vital interests of the data subject or tasks carried out in the public interest.

4.2 Legal basis for processing special categories of personal data

Certain special categories of personal data are afforded extra protection and should not be processed by NCG Group AB except under specific circumstances. Such personal data is personal data that reveals racial or ethnic origin, reveals political opinions; reveals religious or philosophical beliefs; reveals trade union membership; concerns an individual's health; concerns an individual's sex life or sexual orientation; and certain forms of biometric data.

When special categories of personal data is processed for any reason, higher levels of data protection are necessary and in some cases, data protection impact assessments must be conducted.

4.3 Direct marketing

When carrying out direct marketing NCG Group AB must ensure that there is a legal ground for the processing of personal data, that data subjects receive sufficient information about the processing, and that data subjects are able to exercise certain rights such as the right to object/opt-out, right to access, right to rectification, erasure, and restriction.

5. Data subject's rights and information to data subjects

The GDPR gives data subjects a number of rights as regards the processing of their personal data. NCG Group AB must observe those rights and ensure that adequate procedures are in place to accommodate data subjects.

Enquiries by data subjects to exercise their rights must be dealt with swiftly and the NCG Group AB must act on an enquiry within one month after it was received. The time limit may, if necessary, be extended by two months if the NCG Group AB informs the data subject of the extension and the reason for the delay at the latest one month after the request was received. The NCG Group AB is under a duty to take all reasonable actions to check the identity of the data subject.

An enquiry received by any employee of the NCG Group AB should always be immediately forwarded to Country manager/Group CEO for further action.

<i>Right to information</i>	Data subjects have the right to information when the personal data are collected.
<i>Right of access</i>	Data subjects have the right to receive a confirmation of whether or not their personal data are being processed by the NCG Group AB and, if so, gain access to their personal data by receiving a copy of the personal data that are processed (often referred to as a data subject access request).
<i>Right to rectification, erasure ('right to be forgotten') and restriction</i>	Data subjects have the right to have inaccurate or incomplete personal data concerning them rectified or supplemented without undue delay. In some cases data subjects have the right to request erasure of their personal data ('right to be forgotten'). Examples of this are when consent is the legal basis for the processing and the data subject withdraws their consent or if the data subject demonstrates that the data are no longer necessary for the purposes for which they were collected.

In certain circumstances data subjects can demand that the processing of their personal data be restricted. This means that NCG Group AB may only store the personal data and not process them further without the data subject's consent. The right to restriction applies, among other things, when the data subject considers that the data are inaccurate, and has requested they be rectified. The data subject can then request that the processing of the personal data be restricted while their accuracy is ascertained. The individual must be informed when the restriction ends.

Right to object Data subjects have the right to object to NCG Group AB's processing of personal data when the processing is based on NCG Group AB's legitimate interest. When a data subject objects, NCG Group AB must cease processing unless it can demonstrate legitimate grounds that outweigh the rights of the data subject. When personal data are processed for direct marketing purposes, data subjects have the right to object at any time to processing of their personal data. If a data subject opposes processing of personal data for direct marketing purposes, processing for such purposes must cease.

Right to data portability Data subjects have the right to transmit personal data they have provided to the NCG Group AB to another controller (the right to data portability) if the processing is based on contract or consent, and is carried out by automated means. The personal data must be provided to the data subject in a structured, commonly used and machine-readable format. If it is technically feasible, the data subject can request that the data be transmitted directly to another controller. The right applies solely to personal data that the data subject has provided to NCG Group AB.

There are some exceptions where NCG Group AB is not obliged to accommodate a request as described above for example if such a request would conflict with NCG Group AB's legal obligations.

6. Record of processing activities

In accordance with GDPR, NCG Group AB maintains a record of all processing of personal data carried out at the NCG Group AB. The record must contain certain information, such as a description of the categories of personal data and the legal basis for, and purpose of, the processing. On request, the record must be submitted to the relevant data protection authority or other relevant data protection authorities.

7. Data breach procedure

A personal data breach is a security incident that results in accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data that NCG Group AB transmits, stores or otherwise processes (e.g. as a result of hacking, a integrity sensitive email to the wrong recipient or an error in a system that causes data to be lost). If a personal data breach occurs that may result in a risk to the rights and freedoms of private individuals, NCG Group AB must report this to the relevant data protection authority or the relevant data protection authority as required by applicable legislation no later than 72 hours after the breach is

discovered, and in some cases also inform data subjects. When the personal data breach is likely to result in a high risk to individuals, NCG Group AB shall also communicate the data breach to the individuals without undue delay.

Please note that NCG Group AB may also need to notify other third parties of a data breach, such as insurance companies and relevant parties in accordance with contractual obligations

8. Use of data processors and international data transfers

Whenever NCG Group AB enters into a relationship with a third party involving the exchange or transfer of personal data, NCG Group AB must enter into a written agreement with the third party. This helps to ensure that whoever is processing the personal data does so in a legally compliant and responsible manner.

Whenever NCG Group AB exchanges or transfers personal data to a third party that will have the role of a processor, this must be subject to a data processor agreement containing certain requirements. The processor may only process personal data on behalf of NCG Group AB according to the instructions laid out in the processor agreement.

NCG Group AB must ensure adequate protection measures when transferring personal data outside of the EU/EEA. This can be done through one of the following routes:

Option 1 *Transfers on the basis of an adequacy decision* Personal data can be transferred outside of the EU/EEA if the country or entity to which it is being transferred is deemed to have adequate protection by the EU Commission.¹

Option 2 *Appropriate safeguards* If Option 1 is not available, the Company should sign an agreement with the non-EU/EEA party using the EU Standard Contractual Clauses for international transfers (the “SCC”)². Prior to entering into the SCC, NCG Group AB must examine the circumstances surrounding the transfer to a non-EU/EEA recipient, as well as assessing the adequacy of personal data protection in the importing country and document the assessment in a transfer impact assessment (“TIA”). If the TIA reveals that the importing non-EU/EEA country is deemed to have an inadequate protection for personal data supplementary measures (legal, technical or organizational) must be put in place (in addition to SCC).

Option 3 *Specific derogations* If Options 1 or 2 are not used, personal data can be transferred outside of the EU/EEA if a special legal exception (or “derogation” as it is called) applies. Examples of such specific derogations are:

¹ The EU Commission has so far recognised Andorra, Argentina, Canada (commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, South Korea, Switzerland, the United Kingdom and Uruguay as providing adequate protection.

² The SCC are available in four Modules (Controller-Controller, Controller-Processor, Processor-Processor and Processor-Controller). The SCC are available here: https://commission.europa.eu/publications/standard-contractual-clauses-international-transfers_en.

- (a) explicit consent from the data subject after having been informed of the possible risk of such transfer due to the absence of an adequacy decision or appropriate safeguards;
- (b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request; or
- (c) the transfer is necessary for the establishment, exercise or defence of legal claims.

9. Privacy by design and privacy by default

NCG Group AB must ensure compliance with applicable data protection legislation (including GDPR) each time personal data are processed. This means that when IT systems and procedures are formulated NCG Group AB must take appropriate technical and organisational measures to meet the requirements of GDPR and protect the rights of the data subject ('privacy by design'). NCG Group AB must also ensure that, in standard cases, personal data are not processed unnecessarily, and are not made available to an unlimited number of private individuals ('privacy by default').

10. Data protection impact assessments

Even if there is a valid legal ground to process personal data, NCG Group AB must first conduct a data protection impact assessment if it wishes to engage in data processing activities that are likely to result in high risks to the rights of freedoms of individuals (e.g. installing camera surveillance in office areas). A data protection impact assessment is a process to help identify and minimise the data protection risks of a processing activity. Please contact Country manager/Group CEO for more information and/or instructions.

11. Personal data on social media platforms

Whenever NCG Group AB has accounts on social media platforms (e.g. Facebook, Instagram, Twitter, YouTube, etc.) for communication and marketing, it acts as controller for processing of personal data on its own accounts to the extent that NCG Group AB is in control of such publications and has the possibility of making adjustments/delete such information.

Whenever NCG Group AB uses tools provided by a social media platform, e.g. marketing or analytics tools, there is often a joint controllership between NCG Group AB and the social media platform.

To the extent that NCG Group AB is controller, it is required to ensure that its processing activities comply with the content in this manual.

12. Use of cookies on websites and apps

NCG Group AB, as a website or app owner, is responsible for providing users with appropriate information and collecting consent before using cookies to collect, store or process personal data.

Whenever NCG Group AB uses cookies on its websites or apps, it must have and provide a cookie policy. The cookie policy must be available on the website or app and must contain information to the user of the purposes for which cookies are used (e.g. marketing, statistic or functional cookies), how the information collected about the user is processed and if the information is shared with any third parties.

In addition to a cookie policy, websites and apps must have a banner or pop-up form that informs users of NCG Group AB's cookie policy and asks users to consent (or reject) to the use of cookies. The consent must be specific for each purpose, and the user must consent to each specific use.

13. Implementation

13.1 Responsibilities and organisation

Each employee, manager, executive officer and member of the board of directors must understand and comply with this Data Protection Policy. Managers should ensure that their teams fully understand and are expected to comply with the standards and requirements stipulated in this Data Protection Policy.

If you have any questions about the content of this Data Protection Policy, or how it should influence your everyday work or a specific matter, please reach out to Country manager/Group CEO.

14. Reporting concerns and consequences of violation

If you become aware of or suspect a possible violation of law, rule or regulation you are required to promptly contact Country manager/Group CEO.

If you become aware of violation of this Data Protection Policy or any other of NCG Group AB's policies you shall contact Country manager/Group CEO.

You can also raise concerns anonymously through NCG Group AB's whistleblowing system available at [WhistleB, Whistleblowing Centre](#). NCG Group AB will not tolerate any attempt to take adverse action against an employee for reporting a genuine concern regarding suspected wrongdoings. Retaliation against anyone who speaks up will be considered a violation of the Code of Conduct and will not be tolerated

NCG Group AB does not tolerate any illegal or unethical behaviour. Violations of this Data Protection Policy is likely to damage NCG Group AB's brand and reputation. Failure to follow this Data Protection Policy is taken seriously and may result in disciplinary action appropriate to the violation, including, but not limited to, termination of the employment.

15. Review and follow-up

Compliance with this Data Protection Policy by all NCG Group AB entities and employees will be monitored through internal and external audits, and routine follow-ups of all reported matters.

Effective date	Version	Change description
01.09.2023	Ver 1.0	
