Desert Control
GDPR and Privacy Policy for Employees and Former Employees

Document revision:

Date	Revision	# Pages	Revised by	Approved by
8 March 2021	1.1	8	Ole Kristian Sivertsen, CEO	Desert Control Board of Directors
29 January 2020	1.0	6	Ole Kristian Sivertsen, CEO	Desert Control Board of Directors

Desert Control GDPR and Data Privacy Policy for Employees and Former Employees

Table of Contents

INTRODUCTION

As employer, we feel an additional responsibility to protect your personal data. Whether you are a job seeker, are employed by us today or have been in the past, you can rest assured that we value your privacy and that we have taken the necessary steps to align ourselves with the Personal Data Act, including the GDPR.

This Privacy Policy explains how we collect and use (process) personal data in our business. Desert Control AS, by the CEO, is the data controller for the processing.

This Privacy Policy applies to:

Desert Control AS
Business address: Grenseveien 21, 4313 Sandnes, Norway
Org.nr.: 919415630
Email address: post@desertcontrol.com

Desert Control by the general manager, is *the data controller* for personal data where we determine for ourselves the purpose of the processing and the instruments used. The day-to-day responsibilities are further delegated to key people in the organization. Note that the delegation only includes the *tasks* and not the responsibility.

Please read this Privacy Policy first carefully and in particular your privacy rights in the *Your Rights* section below. If you have any questions about your rights or how we process your personal data (such as job seeker or otherwise), we encourage you to contact the Data Protection Officer or your immediate manager.

We take privacy seriously and have taken steps to ensure that we provide clear information about how we process your data and what rights you have. Contact us if you feel something is unclear or missing.

HOW WE COLLECT ABOUT EMPLOYEES

We process (i.e. collect, use, store, record, record) personal data about you at various stages of the "employee journey":

1. When you are in dialogue with us about a position you are interested in
2. When applying for a position (job seeker)
3. Once you have got a job with us (is employed)
4. When you are a former employee

This Statement applies to the processing of personal data concerning you for points 3 and 4 above; when you are employed by us today and what happens to your personal data after the employment has ended.
We do not use automated decision-making or profiling in employment.

OTHER PRIVACY STATEMENTS

For the processing of personal data about visitors to the website, customers (potential, existing and former), contacts and others, see the company's general GDPR and Privacy Policy separately.

PURPOSE AND LEGAL BASIS

An important purpose for us is to run a profitable business to also maintain a safe and stable workplace for our employees. The most common legal grounds for processing your personal data as an employee are in Article 6-1(b) of the GDPR: *necessary to fulfil an agreement in which the data subject is a party, or to take action at the data subject's request before an agreement* and Article 6-1 literal c): *necessary to fulfil a legal obligation that applies to the data controller,* with the legal basis of the Working Environment Act (NO: AML) and the Accounting Act.

Sometimes the legal basis is your consent, but typical for treatments of minor importance, such as signing up for social events or using your image on our websites. Here, of course, you are free to consent to such processing, and you will never experience negative consequences by abstaining from consent.

Read supplementary information on treatments, purposes and legal grounds below.

Your rights

With the Personal Data Act, and in particular the New Data Protection Regulation (GDPR), privacy is stronger than ever before. If you have any questions or concerns about the processing of your privacy, you can contact you at any time to gain access or exercise any of your other rights, as described below.

How long do you have to wait for an answer?

If you wish to exercise one of your rights, you are entitled to a response as soon as possible, and no later than within one month. If we receive many inquiries and/or they are complex in nature, we can extend this deadline by another two months and we will inform you of such a postponement within one month.

PRIVACY RIGHTS

Below you can read about your privacy rights, with links to supplementary information from the Norwegian Data Protection Authority.

Access to your own information

You may request access to any information we process about you and, if necessary, a copy thereof.
Read more about your right to access

Correction of personal data

You may ask us to correct or supplement information that is erroneous or misleading.
Read more about your right to rectified information

Deletion of personal data

In some situations, you may ask us to delete information about yourself (but not always).
Read more about your right to erasure

Restriction of processing of personal data

In some situations, you may also ask us to restrict the processing of information about you.
Read more about your right to restriction

Object to the processing of personal data

If we process information about you on the basis of our duties or on the basis of a trade-off of interest, you have the right to object to this processing.
Read more about your right to protest

Data portability

If we process information about you on the basis of consent or an agreement, you may ask us to transfer your personal data directly to you, or to another data controller.
Read more about your right to transfer information

Complaint to the Norwegian Data Protection Authority

We hope you will speak directly to us if you feel we are not complying with the rules of the Personal Data Act, so we can try to resolve the matter in a good way for you. You can also complain to the Norwegian Data Protection Authority, which will then process the case further. Read about how to do it, here

HOW WE PROCESS YOUR PERSONAL DATA

When you are employed by us, we must process a number of personal data about you, but still no more than what we believe is necessary to fulfil our purposes. We process personal data differently based on where you are in your employee journey.

There may be different:

- types of personal data
- purpose
- legal basis
- systems
- and times of storage and deletion

Below you can read more about what kind of personal data we process, in what systems, where we get it from, how they are secured, and more.

Type of personal data

We typically process your personal data:

- When we create a user for you in our administrative systems, such as employee number, name and email address
- When you travel under the direction of your business, and when travelling abroad, we also record your passport information and your relatives' information
- When you connect to your business's wireless network: Your IP address
- When we communicate digitally with you, such as your name, contact information, and the content of the messages you send
- When you agree that we process your personal data, for example by sharing photos from events you attend, such as on our website and/or social media accounts
- When, in consultation with you, we publish streaming and recording lectures from events
- When you get sick and have to provide self-employment or sick leave, such as your name, employee number, and content in the message
- When applying for vacation, absence, leave, pay increase or facilitation, such as name, employee number, contact information and reason for such applications or facilitation
- When you sign up for our social and professional events, such as your name and email address
- When we log your activity into IT systems and the access control
- In all cases where we otherwise manage your employment, related to, for example, hourly, payroll, expense reports, training, employee conversations, reporting to public authorities and the like
- When we submit applications or required support applications, financing, capital processes, etc. that require the company to share information such as CVs about employees
- When we create a certificate after the end of working conditions, such as name, title, work assignments, and assessment of how you fulfilled your role as an employee

Special categories of personal data

Special categories are personal data about racial or ethnic origin, political opinion, religion, philosophical conviction or union membership, genetic and biometric information, health information, information about sexual relationships or sexual orientation.

The processing of such personal data is initially prohibited, but article 9-2 of the GDPR there are still some exceptions.

In certain situations, we process such information about you, such as if:

1. You need to provide for health reasons and may need to document this by medical certificate. The purpose of the processing is to be able to facilitate the working life for you.
2. You provide self-registration, sick leave or a medical certificate for various reasons. The purpose of the treatment is to be able to process and grant your sick leave, as well as follow you up if necessary (for example, through dialogue meetings with NAV).
3. We ask about allergies or food intolerances at events, where the purpose is to be able to provide safe food for you. Sometimes we need to share this information with third parties, such as by remote catering or if we hold the event outside of school. It is voluntary to provide such information, and we process them only to meet your specific needs.

Our legal basis for processing special categories of personal data for paragraphs 1 and 2 above is Article 6-1(c) of the GDPR); *processing is necessary to comply with a legal obligation*. Article 9-2(b)); *treatment is necessary to fulfil our obligations in the field of employment law in accordance with the law.* Our legal basis for processing special categories of personal data for paragraph 3 is Article 6-1(1) of the GDPR; *consent,* cf. Article 9-2(a)); *your express consent.*

Where do we get your personal data from?

Essentially, we get personal information directly from you, no matter where you are in your employee journey.
We may also collect or obtain personal information about you from:

- Third parties we used in the recruitment process, such as the job seeker portal and the staffing agency
- References you provide
- Testimonials we check
- Former employers
- Unions
- Insurance, pension and travel companies
- Public systems and authorities, such as the Population Register, Altinn and NAV

OUR CORE SYSTEMS FOR EMPLOYEES

We use a variety of core systems to process personal data about employees. For payroll and human resources management, we use Tripletex. Typical personal data processed are names, social security numbers, employee numbers, contact information and information about wages, taxes, account numbers, working hours, sick leave, removal, holiday, leave, travel and reimbursement claims, next of kin, union affiliation and main collective agreement. The personal data here is deleted after the end of the calendar year after the termination of the employment period.

We use *Microsoft 365* as a source system for other IT systems with information about usernames, passwords, email addresses, and group information. Your employee user is created here, as well as all access to other systems.

We use Microsoft SharePoint as an electronic case management and archive system, where personnel folders are stored, among other things. The personnel folder typically contains documents we have received or prepared in connection with your employment (application, CV, etc.) and through the employment relationship (wage changes, leave, personnel matters and more).

The personnel folder is deleted after the end of the calendar year after the termination of the employment.

You can read more about personnel folder at the Norwegian Data Protection Authority

WHO WE SHARE YOUR PERSONAL DATA WITH

To run our business efficiently and profitably, we enter into agreements with and use data processors, partners and suppliers. You can rest assured that we will never disclose or share personal information about you without us having a purpose and legal basis for it.

Sometimes we only disclose your personal data to others once you have consented to it. In other cases, information is disclosed without consent, for example, when we are legally permitted, to fulfill an agreement with you, to public authorities or when it is necessary to perform tasks we are required to perform as a data controller.

We also only share personal data that is essential and/or that we are required by law to share. We quality ensures all data processors we use, for example by entering into data processing agreements. Where we share personal data about you stored outside the EU/EEA, we also collect the necessary guarantees (e.g. EU standard contracts). Suppliers and partners must sign confidentiality declarations and security procedures as needed.

WHAT HAPPENS TO YOUR PERSONAL DATA WHEN YOUR EMPLOYMENT IS ENDED?

If you leave your job with us, we will usually no longer have a purpose in processing your personal data. As a general rule, we delete the personal data of former employees after the end of the calendar year after the termination of the employment period. In some cases, however, we may continue with some treatment, for example if there has been a conflict in the workplace where we have to protect our business legally.

WHAT HAPPENS TO YOUR PERSONAL DATA IF SOMEONE DIES?

If we receive information that a person we process the personal data of is dead, we will delete all information we have about them. However, personal data we are legally required to process, for example related to bookkeeping, we must continue to store.

SAFETY AND RISK MANAGEMENT

We take information security seriously and we will always do our utmost to safeguard your personal data in the best possible way. Among other things, we use strong passwords, encryption of data, access control, backup and two-factor authentication to secure our data and prevent unauthorized users from seeing, modifying, deleting or in any way affecting the data we hold, including your personal data.

We only use reputable IT and management service providers such as web hosting, website and PC security, virus software, email provider, backup, and more. We only allow others to access and/or process your personal data in accordance with our instructions, and only where it is strictly necessary (e.g. for IT support).

You should feel confident that we secure personal data as best as possible. We map and assess the processing of personal data in the business (Article 30 Processing Protocol, for customers, employees and others, and will periodically carry out risk assessment (cf. Article 24 GDPR). Based on such risk assessments, we will, when necessary, update both technical and organizational security measures (cf. Article 32 GDPR) and reduce the risk of discrepancies (e.g. data breaches, hacking, burglary, etc.) as well as possible. Measures are adapted to the type of processing and personal data.

Security measures can be of a technical, physical or organizational nature, and you can see some examples of these below.

Technical and physical safety measures

- Access control for the main entrance at the office (automatic closing and locking of doors outside opening hours), and key system for internal offices
- Access control for printing
- use of strong passwords and two-factor authentication
- encryption of data
- data backup

Organizational security measures

- routines and guidelines for employees (e.g. from the IT department)
- risk assessments of new systems
- quality assurance of data processors, including the collection of data processing agreements and any necessary warranties
- guidelines for what data processors and suppliers access personal data with us, for example, when external IT help is needed
- training, competence and culture

TRANSFER OF PERSONAL DATA OUTSIDE THE EU/EEA

In some cases, your personal data is transferred outside the EU/EEA, for example, where we use suppliers outside the EU/EEA to handle the sending of newsletters, to process customer information, to make available products and services on our website, to enable payment, for security on our website and otherwise in order to operate our business in a safe and efficient manner. The transfer of personal data to outside the EU/EEA is permitted only to countries approved by the European Commission or under the necessary safeguards under the GDPR. For example, these could be the EU's standard contracts.

Due to security, we have not specified these by name. Please feel free to contact us if you would like to know more about which such data processors we use, what kind of necessary warranties apply to such transfer and what additional security measures we have implemented.

PRIVACY IMPACT ASSESSMENT (DPIA)

Article 35(1) of the GENERAL DATA PROTECTION REGULATION states: "If it is likely that a type of processing, particularly when using new technology and taking into account the nature, scope, purpose and context in which it is carried out, will entail a high risk to the rights and freedoms of natural persons, the controller shall, prior to processing, make an assessment of the consequences of the planned processing for the protection of personal data."

In other words, a *data protection impact assessment* (DPIA) is mandatory when processing personal data will entail a high risk to the rights and freedoms of those with which we process personal data.

As of today, based on said risk assessment, we have not identified anything that would indicate *a high risk* to the rights and freedoms of those to whom we process the personal data. We have thus concluded that a data protection impact assessment pursuant to Article 35 of the GDPR is not required.

COMMITMENT TO GDPR, DATA PRIVACY AND SECURITY

Desert Control is committed to the standards described in this policy and further refer to our Code of Conduct as well as our Third-Party Code of Conduct where requirements in addition to GDPR compliance is described. We commit to:

- Comply with GDPR and the local and international privacy and data protection laws and regulations, including laws and regulations regarding the cross-border transfer of personal information.
- Maintain appropriate procedures, safeguards and controls to secure and protect the confidentiality and integrity of all personal information received from, or processed on behalf of, Desert Control.

REPORTING VIOLATIONS

Desert Control asks that any violations are reported to Desert Control's CEO, or the Chairman, or the Board of Directors to whom contact information is found on the Company webpage.

INQUIRIES AND UPDATES

All inquiries and questions should be addressed to Desert Control's CEO.

Desert Control's Board of Directors may update this GDPR and Data Privacy Policy from time to time.

The Board of Directors
Desert Control AS
Sandnes, Norway, 26. March 2021

Number of pages including signature page: **8**