PRIVACY STATEMENT

INTRODUCTION

In this privacy statement you can read all about how your personal data is collected and how it is handled. It explains where your data is stored and for what purposes it will be used. In addition, you will find all your rights regarding your data and how you can use these rights.

The privacy statement will sometimes be modified by, for example, changes in the law. It is therefore advisable to consult the statement periodically.

NOSUCH

You are currently reading the privacy statement of NOSUCH, a results-driven creative agency focused on branding, content and creative lead generation.

There are situations in which your data is collected by NOSUCH. It is therefore good that you know what is done with it and how you can indicate your wishes regarding your data. That is what this statement is about.

If you don't feel comfortable with the use of your data by NOSUCH, please contact us!

NOSUCH
Schiehavenkade 214-222, 3024 EZ ROTTERDAM
privacy@nosuch.nl
0031 10 2441044

PURPOSE OF DATA

Personal data is collected by NOSUCH for several purposes. In doing so, the principle of data minimization is strictly followed. This means that only the minimally necessary personal data is collected and processed for each specific purpose. We never request or store more data than is needed to carry out the relevant service or activity.

1. Sending out Newsletters

NOSUCH sends newsletters via e-mail. These newsletters are commercial on the one hand and aimed at knowledge sharing on the other. Your name and e-mail address will be collected through the appropriate form on the website of NOSUCH. In addition, you may be asked verbally or textually to sign up for the newsletter.

1. Sharing Marketing Material

NOSUCH sends marketing material on request. Your data is collected when you make known via the website of NOSUCH that you would like to receive marketing material. This includes your name, e-mail address, company name, function within your company and the address details for sending.

2. Contacting NOSUCH

Your data will be collected if you contact NOSUCH via the website. However, this form only asks for the data necessary to provide a proposal or service, such as your name, e-mail address, company name, phone number and description of your question or request.

3. Analytics

The website of NOSUCH collects your data to improve the website. This is done with Google Analytics. This data is anonymous and not linked to your personal data. Think of information such as the duration of your website visit or the pages you visit.

4. Applications

Through the website there is a possibility to apply directly. We ask for your name, e-mail address, telephone number and CV. Additional information is provided voluntarily. Your data will only be used within the selection process of the relevant vacancy.

All data will only be processed with your explicit permission, or for the execution of the agreements entered into, or on the basis of legal obligations.

DATA MINIMIZATION AND PROPORTIONALITY

NOSUCH adheres to the following principles for data minimization:

1. Minimal Requirements: For each processing activity, only the data strictly necessary for the intended purpose is collected. Unnecessary data collection is actively avoided.
2. Protecting Rights and Freedoms: When collecting and processing personal data, NOSUCH continuously assesses whether the amount of collected data is proportional to the rights and freedoms of the individuals involved.
3. Evaluation of Collected Data: NOSUCH conducts periodic checks to ensure that only the necessary data is collected and processed, in line with the objectives described in this document.
4. Removal of Unnecessary Data: Personal data that is no longer needed for the intended purposes is immediately deleted or anonymized, unless there is a legal obligation to retain the data for a longer period.

RECEIVERS

The data that NOSUCH receives and processes is managed through:

1. Campaign Monitor

The newsletters are sent out with Campaign Monitor. When you sign up for the newsletter, your email address and name are automatically stored in the appropriate list within Campaign Monitor.

2. Microsoft Office365

The e-mail of NOSUCH is hosted by Office365. The moment you contact us via the forms or e-mail, the e-mails in question are stored on the Office365 servers.

3. Savvii

The website and backups of the website of NOSUCH are hosted by Savvii. Data that you leave on the NOSUCH website is stored on Savvii's servers.

4. SCORO

NOSUCH performs project and financial administration in SCORO. The minimum information needed to manage a project and process the purchase and sales invoicing is stored there.

5. Loket en XpertSuite

The personnel administration is carried out in Loket. This contains all the personal data of our employees. The Occupational Health and Safety Service works with XpertSuite for absence management.

6. Recruitee

Applications come in to Recruitee, here the entered data is stored in profiles.

7. Central Network

Information that cannot be stored in a system, but must be kept, is stored as a file on a central network drive on Microsoft Windows Server.

8. Hubspot

NOSUCH uses HubSpot for customer management (CRM), marketing automation, and contact follow-up. When you subscribe to newsletters or show interest in our services through the website, your personal data such as name, email address, company name, and phone number are stored in HubSpot. This data is used exclusively for communication and marketing activities for which you have explicitly given consent.

9. Business Monitor

NOSUCH uses Business Monitor for customer and employee satisfaction surveys. Personal data such as names, email addresses, and feedback are collected and analyzed to gain insights that help improve customer experience and internal processes. Business Monitor provides secure storage on Dutch servers and offers real-time analytics and reporting to make results transparent and optimize them.

PERIOD OF RETENTION

Your data will be kept by NOSUCH for a longer period of time, but never longer than is necessary for the execution of activities, unless we have to keep your data longer by virtue of a legal regulation.

1. Sending out Newsletters

Your email address and name will be stored in Campaign Monitor. The storage of your data is indefinite. You can unsubscribe at any time using the link at the bottom of the newsletters or by sending an email to privacy@nosuch.nl. Your request will be dealt with within 2 working days.

2. Sending out Marketing Material

Your email address, name, company name, position and address details are stored in Campaign Monitor. The storage of your data is indefinite. You may unsubscribe at any time by sending an email to privacy@nosuch.nl. Your request will be dealt with within 2 working days.

3. Contacting NOSUCH

The moment you contact NOSUCH via mail, the data you send, such as your name, company name and e-mail address will be stored on the mail server. The storage of these mails is indefinite. If you would like to have your e-mails removed from this mail server, you can make this request via privacy@nosuch.nl. Your request will be followed up within 2 business days.

4. Analytics

The data that Google Analytics collects on the website is anonymous, i.e. not linked to your name, company or email address. This data is stored indefinitely within Google Analytics.

5. Recruitee

When you apply for a job, you give permission for a retention period of 6 months. After these 6 months your profile will be deleted, unless otherwise agreed.

6. Hubspot

Personal data collected through HubSpot, such as name, email address, and contact information, are stored as long as they are needed for customer relationship management, marketing activities, and communication. The data will be deleted or anonymized once they are no longer relevant for these purposes, with a maximum retention period of 5 years, unless otherwise required by law or if the individual requests deletion.

7. Business Monitor

Data collected via Business Monitor, such as name, email address, and feedback, are stored as long as they are needed for analyzing customer and employee satisfaction and for optimizing services. The data will be deleted or anonymized once they are no longer relevant for these purposes, with a maximum retention period of 5 years, unless otherwise required by law.

SECURITY

No physical copies are made of your personal data. Your data is only managed in the aforementioned systems and software. Exceptions to this, such as copies required to comply with legislation, are kept in a locked room and are only accessible to authorized employees.

Personal data managed by NOSUCH or by previously mentioned third parties is only accessible through the above software and is password protected.

The devices that access your data are each themselves also locked with a password and/or fingerprint. The number of devices that have access to your information is limited to only the necessary ones.

In addition, your visit to our website is secured by an SSL certificate. This means that your connection to the website of NOSUCH is private. You can recognize this security by the green lock in front of the url.

In the attachment you will find the Data breach protocol, as drawn up by NOSUCH and shared with the employees and processors of our data.

YOUR RIGHTS

1. Right to Inspect

You have the right to request at any time your data that is recorded and stored at NOSUCH. You can do this by sending an e-mail or contacting NOSUCH by telephone. You will then receive an overview of your data.

2. Right to Rectify

Is your data not correct? Or has your data changed? You have the right to have this corrected by NOSUCH. You can change your data concerning the newsletter via the appropriate url at the bottom of each mail.

3. Right to Transfer

If you need the data stored at NOSUCH in case you switch to another party or service, you have the right to transfer. NOSUCH will then have to transfer all your data to the other party.

4. Right to Delete Data

Do you no longer want your data recorded at NOSUCH? Then you have the right to have your data erased.

5. Right to File Complaint

You have the right to file a complaint with the Dutch Data Protection Authority, if you feel that NOSUCH does not handle your data in the right way. You can do this via this link.

6. Right to Stop Using Data (Complaint)

Do you not want NOSUCH to use your data? Then you have the right to stop the use of your data.

You can exercise these rights by sending a copy of your ID-card to privacy@nosuch.nl, in which the passport photo, ID-number and BSN are made unreadable. We aim to respond within 5 working days.

DUTIES

NOSUCH processes personal data based on a legitimate interest. For example, offering services or products from NOSUCH via e-mail. Your data will never be sold to third parties. Similarly, other processing is necessary to carry out our business activities.

The data that are required to be provided are the minimum data necessary to offer services or products. For example, your e-mail address is required to send the newsletter. If this mandatory data is not provided, NOSUCH cannot offer the service in question.

Should it be necessary to share the data you have shared with NOSUCH with others than the above-mentioned parties (for example to offer a service), your permission will be asked first.

NOSUCH reserves the right to disclose the data when required by law or when NOSUCH deems it justified to comply with a legal request/process or to protect the rights, property or safety of NOSUCH. We always try to respect your right to privacy as much as possible.

Do you still have questions? Please contact us via the contact details below.

NOSUCH
Schiehavenkade 214-222, 3024 EZ ROTTERDAM
privacy@nosuch.nl
0031 10 2441044

PROTOCOL DATA BREACHES

ARTICLE 1 - DEFINITION DATA BREACH

A data breach occurs if there has been a breach of personal data. A threat or security flaw is not a data breach; personal data must have actually been leaked.

The AP understands a data leak to mean personal data that has been leaked or destroyed as a result of a security incident. In the event of the leak, personal data are exposed to loss or unlawful processing.

In case of loss, the personal data is no longer there. Unlawful processing includes, for example, unauthorized access, modification, impairment or disclosure.

ARTICLE 2 - POINT OF CONTACT

Client and data processor shall designate a contact person to whom any data breaches should be reported. This could be, for example, a board member or the Data Protection Officer (hereinafter: 'Contact Person' or 'Contacts').

ARTICLE 3 - INFORMING EMPLOYEES

Employees within the organization must immediately report any (suspected) data breach to their supervisor and the designated Contact Person. If the Contact Person is not immediately available, the incident should also be reported to a backup contact person or the Data Protection Officer (DPO). Supervisors are required to escalate any report of a data breach to the Contact Person within one hour, ensuring that the breach can be assessed within 72 hours and, if necessary, reported to the Data Protection Authority (AP). They must be familiar with the Action Plan outlined in this protocol (ARTICLE 4).

ARTICLE 4 – ROADMAP

PROCESSING STEPS	ACTIVITIES	RESPONSIBILTIES
1. A (POSSIBLE) DATA BREACH IS ENCOUNTERED	Upon discovering a (potential) data breach, the employee must immediately report it to their supervisor and the Contact Person. If no confirmation of receipt is received within 1 hour, the employee should contact the Data Protection Officer (DPO).	Employee who discovers the data breach
2. ASSESMENT OF THE DATA BREACH	- Investigate the security incident - Investigate whether personal data has been lost or may be used unlawfully - Assess who or what departments within the organization are involved	Manager of the substantive department involved Manager of the department responsible for security incidents (for example: IT) Contact person(s)
2A. ESCALATION IN CASE OF UNCERTAINTY	If the scope or impact of the data breach is unclear, the supervisor must escalate the issue to the Data Protection Officer (DPO) within 1 hour for further assessment.	Supervisor Contact person(s) Data Protection Officer (DPO)
3. COUNTERING THE DATA BREACH	- Stop the data breach if you still can - Take other measures to mitigate the data breach and consequential damage - Document the actions taken	Manager of the substantive department involved Manager of the department responsible for security incidents (for example: IT) Contact person(s)

4. DETERMINING THE IMPACT	- Investigate the data breach and its consequences - Investigate the nature of the data that was leaked. For example: health data, passwords, financial situation data or data that could lead to stigma/abuse - Investigate the extent of the leaked data - Assess what impact the leak may have on data subject(s) - Determine what the adverse effects may be	Manager of the substantive department involved Manager of the department responsible for security incidents (for example: IT) Contact person(s) Data Protection Officer
5. DETERMINIG REPORT- AND RECOVERY APPROACH	- Determine approach/inform AP - Determine approach/inform data subject(s) - Determine actions for aftercare data subject(s) - Define actions for the interest of the organization - Define actions for improving security	Manager of the substantive department involved Manager of the department responsible for security incidents (for example: IT) Contact person(s) Data Protection Officer
6. REPORTING AT AP *)	- If it is decided to inform the AP, this must be done within 72 hours - Notification via the website of the AP - The data breach notification form can be used in advance	Contact person(s) Data Protection Officer Board

7. INFORMING INVOLVED DATA SUBJEC(S) **)	- Notification by letter, for example - Inform the person concerned of what has happened, what personal data has been affected and what the possible consequences of the data leak are. - Inform about the measures that the organization is taking and that the person involved can take themselves to prevent damage	Contact person(s) Data Protection Officer Marketing/Communications Board
8. REPARATION	- Recover the data breach - Improve security - Provide aftercare to data subject(s)	Manager of the department responsible for security incidents (for example: IT) Contact person(s).
9. OPTIMIZING THE PROCESS	Record, evaluate and improve security, improve process, including this protocol	Contact person(s) Data Protection Officer Board Manager of the department responsible for security incidents (for example: IT)

*) Notification to the AP may only be omitted if it is unlikely that the data leak will result in an increased risk to the rights and freedoms of the data subject(s). Whether this is the case depends in part on the nature, context and extent of the personal data leaked. For example, if only the address details of a small group of data subject(s) have been leaked, it is unlikely that there is an increased risk. Also consider the context. For example, if only address data has been leaked, but in combination with traceable membership of a patient or client organization, this may be a sensitive piece of data. When weighing up the risk to the rights and freedoms of data subject(s), the Data Protection Officer should always be involved.

**) If it can be assumed that the data breach leads to an increased risk to the rights and freedoms of data subject(s), it must also be reported to data subject(s). The risk must be assessed on the basis of the nature and quantity of the leaked data. If special personal data has been leaked, the leak must be reported to the data subjects in all cases. When considering the risk to the rights and freedoms of data subject(s), the Data Protection Officer should always be involved.

ARTICLE 5 - DATA PROCESSOR

Client is and remains (as data controller) always ultimately responsible, even if the data leak occurred at data processor. This means that also in this case the same step-by-step plan must be completed. Data processor must be involved in all relevant steps.