

WHAT PERSONAL DATA WE COLLECT – OTHER

29 oktober 2025

Tabel overzicht

Purpose/Activity	Personal Data Processed	Lawful Basis for Processing	Retention Period	How do we receive the personal data	Transfer of personal data to third countries
Audits We may be subject to audits for certifications or by our customers or conduct internal audits to verify if we comply with our various requirements. If we process your personal data, this personal data may be processed by the auditor if this is strictly necessary for the audit. We will anonymise or pseudonymise your data as much as possible before sharing it with the auditor Your personal data may be shared with the auditor	All personal data described in this privacy statement may be included in the audit, but only insofar as necessary	- Compliance with a legal obligation to conduct audits - Our legitimate interests to operate our business, to be able to comply with contractual agreements concluded with customers, to (verify that we) comply with legislation, to gain certifications and to verify that we comply with modern security requirements	We store the personal data for up to 2 years after the audit took place or, if storing personal data is an audit requirement, for up to 2 years after expiry of such term	This depends on the type of personal data we processed. This is described per type of personal data in this table	No
Back-ups We create back-ups of our data. This will also include your personal data if we process your personal data. This data is stored	All personal data as described in this privacy statement	- Compliance with a legal obligation to create back-ups - Our legitimate interests to operate our business, to be able to comply with contractual agreements concluded with customers, to comply with legislation	We store the personal data for up to 7 years after the back-up has been created, except in case of an incident for which the back-up is required in which case the back-up will be stored until	This depends on the type of personal data we processed. This is described per type of personal data in this table	No

encrypted and is not generally accessible. We will only use a back-up in case there is an unintended loss of data which cannot be solved in another way		and to prevent unnecessary loss of data	the incident has been handled		
Security and monitoring We take various measures to secure our services and the data that we process. We scan incoming e-mail to detect threats (e.g. viruses and phishing), we have a secure file exchange and we register visitors to our offices	E-mail scanning: - E-mail address - Metadata of the e-mail (e.g. date of sending the e-mail) - Content of the e-mail Secure file exchange: - Shared files - E-mail address - IP address Office visitors: - Name - Employer - Signature	- Compliance with a legal obligation to secure our networks, software and data - Our legitimate interests to operate our business, protect our networks, software and data and to fulfil our contractual obligations towards our clients and our legal obligations	E-mail scanning is done automatically and personal data is stored for up to 1 year after the e-mail has been scanned We store the personal data for the secure file exchange for up to 14 days after the exchange has taken place We store the personal data for office visits for up to 6 months after the visit has taken place	In case of e-mail scanning and the secure file exchange, we gather the personal data from our systems. In case of office visitors, the personal data is received from you directly or from one of your colleagues	No
CCTV We may record images of you via CCTV if you visit and access Ctac's locations	- The recording - Metadata related to the recording (e.g. location and timestamps)	Our legitimate interest in complying with our legal obligation to secure our services and (sensitive) data and being able to secure your and our services, data, locations and property and to investigate incidents	For up to 30 days after the recording has been made. In case of an incident, the relevant recordings will be stored until the incident has been handled	The recordings are generated by the cameras of Ctac	No
Incident investigation	All personal data described in this privacy statement may be	Necessary to pursue our legitimate interest in	In case of an incident, the personal data processed for	As described in this privacy statement for	No

If an incident has occurred, Ctac may process your personal data if this is relevant for the investigation or handling the incident	included in the investigation, but only insofar as necessary	being able to investigate incidents	investigating and handling the incident will be stored until the incident has been handled	the various personal data	
Government requests and court orders We may receive requests from government authorities or court orders which oblige us to share your personal data with them or a party designated in the order. We will inform you of such orders prior to sharing your personal data, unless the order forbids us from doing so Your personal data may be shared with the authority, court or other party designated in the order	All personal data described in this privacy statement may be included in the request, but only insofar as Ctac is obliged to provide the personal data	- Compliance with a legal obligation to comply with the order - Our legitimate interests to be able to comply with lawful orders and legislation	We store the personal data until the order has been fulfilled and any terms of appeal or objection have expired	This depends on the type of personal data we processed. This is described per type of personal data in this table	No, unless the entity with whom we must share your personal data is located outside of the EEA. The transfer mechanism upon which we will rely depends on the entity with whom we share your personal data and the country in which the entity is located.
Mergers and acquisitions If we process your personal data, we may also process your personal data if we	All personal data described in this privacy statement may be processed to successfully complete the transaction, but only insofar this is necessary	Our legitimate interests to operate our business, to be able to comply with contractual agreements concluded with other parties,	We store the personal data for up to 5 years after the transaction has been completed or for the duration of relevant indemnities and	This depends on the type of personal data we processed. This is described per type of	No, unless the other party is located outside of the EEA in which case we will rely on an adequacy decision of

merge with another company, if we acquire another company or if we are acquired by another company. Your personal data will only be processed if this is strictly required for the transaction or the due diligence investigation. In such cases, we will anonymise and pseudonymise your personal data where possible Your personal data may be shared with the target company or purchaser, involved lawyers and accountants and other parties involved in the transaction Due to the confidential nature of the processing activity, you will not be informed separately prior to your personal data being processed for this purpose. Insofar as we are allowed to	to achieve the desired result. If possible Ctac will anonymise your personal data	to comply with legislation and to prevent unnecessary risk and damage from occurring to Ctac or other parties	warranties for which your personal data is crucial to be able to invoke or defend against such warranties and indemnities	personal data in this table	the European Commission. If such an adequacy decision is not available, we will rely on standard contractual clauses and conduct a transfer impact assessment to verify if the transfer is allowed under the GDPR When you are informed about the processing activity and the transfer is based on standard contractual clauses, you may request access to those clauses and our transfer impact assessment by contacting us via the contact details included in this privacy statement
---	--	--	--	------------------------------------	---

do so, we will inform you afterwards					
Conflict management If there is a (legal) conflict of which you are an essential part and we process your personal data, your personal data may be processed if necessary for settling and managing the conflict. For example, if you are the employee or representative who negotiated the contract on behalf of the customer with whom we have a conflict Your personal data may be shared with involved lawyers, courts and other involved judicial professionals (e.g. the bailiff) if necessary for resolving the conflict	All personal data as described in this privacy statement, insofar as necessary for settling the conflict	Our legitimate interests to be able to manage and settle conflicts and to exercise our rights	We store the personal data for up to 7 years after the conflict has ended and all obligations of parties have been fulfilled If the conflict has been settled by a court and a judgment has been given, the personal data will be stored for the limitation period	This depends on the type of personal data we processed. This is described per type of personal data in this table	No
Complying with GDPR requests You may exercise your rights under the GDPR. We	Personal data to identify you. The specific types of personal data we process to identify you depend on the personal data we have available	- Compliance with a legal obligation to comply with GDPR requests - Our legitimate interests to comply with our legal obligations	We store the personal data for up to 2 years after the request has been fulfilled	This depends on the type of personal data we processed. This is described per type of	No

must process your personal data when complying with your request. We will only process the personal data which is necessary to comply with your request	(such as your name and e-mail address) • All personal data as described in this privacy statement, insofar as necessary to comply with your request			personal data in this table	
---	--	--	--	-----------------------------	--