Version: 1.0 E

Date: August 7, 2024

M365 Data Processing Information

TABLE OF CONTENTS

Information about consent, recordings or transcriptions of team meetings are under section 10 below

1. INTRODUCTION

These Data Protection Information (“Information”) is for anyone who is working on Exyte Microsoft 365 systems (including e-mail system, OneDrive, Microsoft Office, the Document Management and Control System, i.e. DMCS as well as oneNET). This may be among others, if you are an employee, with an Exyte account or a consultant, supplier, customer, client or otherwise conduct business to us (“Business Partner”). Furthermore, you may have gotten this information because you are working for a Business Partner.

For further information on how we process your personal information, please also see the following links:

- As Business Partner: Personal data processing for customers | Exyte
- As employee: Employee Data Protection (sharepoint.com)

Please note that this Information covers mostly personal data (“Personal Data”) which are processed in the frame of providing the Microsoft 365 platform, i.e. to enable users to collaborate in a safe and stable system. We may process content , which is created in the M365 System (e.g. content of a word document or an email, which created by a user) – following referred to as “Content Data” as well. Processing of Content Data mostly occurs in the frame of the services, i.e. when you store a document or send an email via our systems, but may also e.g. in the frame of an eDiscovery (see below). In such cases the Personal Data depend on the Personal Data you enter into the Microsoft 365 platform.

We may provide you with other data protection information as needed if we process personal data about you as Content Data on the M365 Plattform.

If you are an employee of a German Exyte entity the following works council agreements apply to you in addition (subject to applicable changes):

- KBV IT Systeme
- KBV Outlook / Exchange
- KBV M365

The above are referred to as “Workers Council Agreements” or “WCA”.

This Information are for your information only and the Information do not constitute a contract or a claimable right against Exyte. Rights can only be derived from the applicable laws.

In case the controller responsible for you is an entity outside the EEA and the GDPR does not apply to processing your Personal Data by the entity, the legal basis and rights as named in these information do not apply to you. However, as long as applicable law does not state otherwise the information applies to you respectively and we will provide you with the same information, however based on our discretion and without obligation.

For the purpose of this information we separate the following:

Personal Data	Any information relating to an identified or identifiable natural person (data subject). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
Private Information	All information, which are not related to your work at or your business relationship to Exyte.
Personal Work Information	All Information which is data, that is personally related to the situation of the User in the context of the work at Exyte, e.g. contract negotiations between Exyte and an employee, complaints to the compliance department, complaints and communication with and at the HR Department; The definition also applies to communication between Users sharing Private Work Information about a third user, e.g. Compliance or HR Personal sharing the information among each other.

It is strictly prohibited to use the Microsoft 365 platform for any private purpose or to load any private information.

Employees of Exyte entities are permitted to use the Microsoft 365 platform for processing personal work information.

2. Name and contact details of the Controller

The controller of your Personal Data in the Microsoft 365 platform is the entity you have a contract as employee or Business Partner with.

If you are engaged by a Business Partner of Exyte the Controlling entity is the contract partner of the business partner.

If you are unclear about the controlling entity, you can always turn to the DPO of Exyte Management GmbH (No 4 below). The DPO will provide you with the required information.

The contact data of the Exyte Management GmbH are:

Exyte Management GmbH

Phone: +49(0) 8804-0
info@exyte.net

www.exyte.net

The controller is referred to as “we”, “us” or “Exyte”.

3. Additional information about the Microsoft 365 platform and cookies

Exyte Management GmbH is managing the Microsoft 365 platform for all other group members as processor. The Exyte Group members have concluded a Data Processing and Joint Controller Agreement (DPJCA) to keep your data safe.

Exyte engages other group members and third parties as sub-processors or for other services to provide the Microsoft 365 platform for the Exyte Group, such as Microsoft Ireland Ltd.

The Microsoft 365 platform encompasses all M365 services, including SharePoint, OneDrive, Exchange, Outlook, Teams, Microsoft Office applications, and other Microsoft 365 applications.

In this regard, if you have questions regarding how your data are processed you can always approach Exyte Management GmbH directly. Exyte Management GmbH will coordinate with the controller and provide you with the required information.

Please further note that the Information are only about how Exyte processes your Personal Data. Microsoft may also process your Personal Data as independent controller, e.g. when using their website or apps. In addition Microsoft may place cookies on your device.

Generally, Microsoft will provide you with separate information on how Microsoft provides you with personal data as controller, where required.

You can also find additional information here: https://privacy.microsoft.com/en-us/privacystatement and for third party cookies under: https://support.microsoft.com/en-us/topic/third-party-cookie-inventory-81ca0c3d-c122-415c-874c-55610e017a6a

4. Data Protection Officer

We have appointed a Data Protection Officer ("DPO"). You can reach the DPO under the following email address: privacy@exyte.net.

Please feel free to contact the DPO in case of any questions, complaints, inquiries, or suggestions regarding processing the processing of Personal Data at Exyte.

5. Data we may process, purpose, and legal basis

The purpose of the Microsoft 365 platform, in general, is to provide a creation, collaboration, and communication method for employees and Business Partners. Along with the aforementioned, there are requirements to process personal data for reasons of security, stability, and safety of the Microsoft 365 platform.

For your convenience we separate the processing in Microsoft 365 into general categories. Please note that the categories below mostly refers to personal data which is processed in connection with the use of the Microsoft 365. We, however, also process content – Content Data - in the frame of e.g. when storing documents, sending emails, using other M365 functionalities to process and create content, eDiscovery actions, searches, or other matters. These Information depend on which information you included in the Microsoft 365 platform. The core reasons for processing such Content Data and how respectively for which purpose such content data is used depends on your individual case, and where necessary we will inform you about such processing in separate data protection information:

No 1	General Processing of personal data in M365
Description	Processing that encompasses the entire M365 platform. In the Numbers below individual processes of services of the M365 System are listed, where they deviate, process additional data, are of particular importance or risk, or specifically transfer additional personal data.
Processed Personal Data	Any data users enter to use the system Basic personal data (for example First and Last name, Email, Job Title, Business Mobile, Business Phone, place of birth, street name and house number (address), postal code, city of residence, country of residence, mobile phone number, first name, last name, initials, email address, gender, date of birth, engaging company, employer), including basic personal data about family members and children, such as:

	• Your Name • Your employer or the company who engaged you; • Additional information you enter into our system about you, including your photo, Email, Job Title, Business Mobile, Business Phone, place of birth, street name and house number (address), postal code, city of residence, country of residence, mobile phone number, first name, last name, initials, email address, gender, date of birth**, engaging company, employer**; • Your email address designated to you by M365; • Your telephone number / your mobile phone; • Identification information in the system (internal ID no); • Furthermore, if you work on files in the M365, we log your information including changes you made to files, when you accessed files, how long you accessed files, information you store and transfer in M365, to whom you transfer such information, how long you logged on, from where you logged on, what time you logged on, etc. • Authentication data (for example name, username, password or PIN code, phone number, user ID security question, audit trail); • Contact information (for example addresses, email, phone numbers, social media identifiers; emergency contact details); • Unique identification numbers and signatures (for example Social Security number, bank account number, passport and ID card number, driver's license number and vehicle registration data, IP addresses, employee number, student number, patient number, signature, unique identifier in tracking cookies or similar technology); • Pseudonymous identifiers; • Investigation Data; • IP Address • Employee Number • Employer • Location data (for example, Cell ID, geo-location network data, location by start call/end of the call. Location data derived from use of wifi access points); • Internet activity (for example browsing history, search history);

	• Device identification (for example IMEI-number, SIM card number, MAC address); • Profiling (for example based on observed criminal or anti-social behavior or pseudonymous profiles based on visited URLs, click streams, browsing logs, IP-addresses, domains, apps installed); • All content data, as you enter them into the M365 platform; • Your status information (Busy, Free, In a call, Absent) and the content you set in absent messages
Usage / Process	General usage in the entire M365 System
Purpose	Provide a worldwide secure and stable data management and exchange system in order to provide business services, exchange information with Business Partner as well as enable users to use the tools in M365. to efficiently work, create content and communicate / collaborate among each other and with others efficiently and enabling Exyte to prevent criminal and incompliant behavior as well as to assert and defend from legal claims.
Legal basis	Art. 88 I GDPR i.c.w. the Workerscouncil Agreement M365 (WCA M365); Art. 6 I b GDPR in order to fulfill contractual requirements, Art. 6 I f GDPR, where it is our legitimate interest to provide a comprehensive secure and efficient working system, to exchange data and information worldwide respectively keeping them safe. Please note that user and other system setup, such as EHS, may process and transfer additional personal data using the M365 platform. We provide information about such processing activities separately, where necessary.

No 2	Microsoft Entra
Processed Data	• First Name • Last Name • Email Address • Job Title • Unique User ID • Business Mobile • Business Phone • Employer, Engaging Entity • IP Address • Basic device information
Usage / Process	Microsoft Entra is used to control the role-based access, and to control identity in the Exyte cloud environment. Any time a service, a location, or content is accessed, Microsoft Entra is confirming the identity of the user and whether the user has the right to access the system.
Purpose	Controlling access to the Exyte M365 environment, identify the user and grant role-based access of the users.
Legal basis	Art. 88 I GDPR i.c.w. the Workerscouncil Agreement M365 (WCA M365); Art. 6 I b GDPR in order to fulfill security requirements as agreed in contracts with other companies to maintain a security level, Art. 6 I f GDPR, whereas the legitimate purpose is to establish a safe system by a role based access and to ensure a stable and safe system as well as to comply with the code of conduct and laws and regulations and to safeguard our claims,.

No 3	Exchange / Teams
Processed Data	• Name, • Email address • The content of your message including sound and picture

	• Data about teams, recipients, groups, message time sent, message time received, etc.; • Service Generated Data to facilitate communication, e.g. Personal Data required to exchange message through the exchange system, i.e. email addresses, time, IP addresses, content in the subject line, etc.
Location	Europe (please note that in case of sending messages and emails to others outside the M365 platform, we lose control over the location as soon as the message is transferred out of our system, based on the instructions of the user (i.e. you)
Usage / Process	Exchange of email messages, calendar messages, and other messages between employees, freelancers, customers, applicants, suppliers, authorities, applicants, and others
Purpose	Communication in the course of business, investigations in compliance, breach of laws or the code of conduct, security and stability of the system and to assert or defend from legal claims
Legal basis	Art 88 II GDPR i.c.w. WCA 365, Art 88 II GDPR i.c.w. WCA Exchange, Art. 6 I d GDPR, Art. 6 I f GDPR legitimate interest, whereas the legitimate interest is communication in the course of the business and to ensure a stable and safe system as well as to comply with the code of conduct and laws and regulations and to safeguard our claims, Art 88 I GDPR i.c.w. Art 26 Bundesdatenschutzgesetz (“BDSG”) for the implementation of a labor contract for employees.

No 4	SharePoint Online, OneDrive and List
Processed Data	File, file metadate, and transfer data including access to files, transfer, and time. The content of the data you store Furthermore, changes and deletion or transfer of individual files.
Usage / Process	Tool for storage, exchange and collaboration of data
Purpose	Storage and transfer of data in the course of business and to ensure a stable and secure system as well as to comply with the code of conduct and laws and regulations and to safeguard our claims and third party (intellectual) property,

Legal basis	Art 88 II GDPR i.c.w. WCA 365, Art 88 II GDPR i.c.w. WCA Exchange, Art. 6 I d GDPR, Art. 6 I f GDPR legitimate interest, whereas the legitimate interest is to store data and communication in the course of the business and to ensure a stable and safe system as well as to comply with the code of conduct and laws and regulations and to safeguard our claims and property, Art 88 I GDPR i.c.w. Art 26 Bundesdatenschutzgesetz ("BDSG") for the implementation of a labor contract for employees.

No 5	M365 / Microsoft Graph
Processed Data	M365 / Microsoft Graph generally tracks all interactions of users in the M365 platform and sorts, assembles, and provides such information to other services in M365, where required or requested by the user.
Usage / Process	All data is analyzed by the graph algorithm in order to filter relevant data and provides relevant information and suggests improvement
Purpose	Improvement of users collaboration and efficiency and to ensure a stable and secure system as well as to comply with the code of conduct and laws and regulations and to safeguard our claims and property.
Legal basis	Art. 88 I GDPR i.c.w. the Workerscouncil Agreement M365 (WCA M365); Art. 6 I f GDPR, whereas it is our legitimate interest to optimize collaboration and work efficiency and to ensure a stable and secure system as well as to comply with the code of conduct and laws and regulations and to safeguard our claims and property,.

No 6	M365 Microsoft Threat Protection, including Cloud App Security, Defender Antivirus and Device Guard, Defender for O365, Defender Portal, Defender for Identity, and security audit log
Processed Data	• User Name, • User ID, • Content Data, • Pseudonymized User ID; • Geolocation Data, • IP Address

	• Pseudonymized user behavioral data • User profile data – log in time, actions on the M365 platform, behavioral abnormalities (e.g. deleting or moving an unusual amount of data) • User Web Traffic • User files • IP Addresses • Location data (for example, , geo-location network data, location by start call/end of the call. Location data derived from use of wifi access points); • Internet activity (for example browsing history, search history); • Device identification (for example IMEI-number, SIM card number, MAC address);
Usage / Process	User behavior is analyzed and logged to identify malicious intrusion into the system. Content and web-traffic (including links) are analyzed to identify malware. User behavior is pseudonymized locally and compared to other user behavior data to identify large cyber-attacks and take preventive measures on a global level. Accounts with suspicious (malicious) behavior a flagged automatically for our IT Staff to take measures from triggering a re-authentication to full block.
Purpose	Improvement of confidentiality and security of the system and to ensure a stable and secure system as well as to comply with the code of conduct and laws and regulations and to safeguard our claims and property,
Legal basis	Art. 88 I GDPR i.c.w. the Workerscouncil Agreement M365 (WCA M365); Art. 6 I f GDPR, where it is our legitimate interest to to ensure the safety and stability of our systems and to ensure a stable and secure system as well as to comply with the code of conduct and laws and regulations and to safeguard our claims and property,.

No 7	M365 Compliance – eDiscovery, Audit and Content Search
Processed Data	All data on Exchange Online, OneDrive, Viva Engage, SharePoint Online locations, and other M365 services
Usage / Process	Search and sorting of personal data

Purpose	Access to important business data and business communication, to find important business data in the frame of communication with business partners, to prepare assertion of claims, to assemble information in order to follow discovery / access orders or legal requests by a court or an authority having jurisdiction and to investigate incompliant or criminal behavior.
Legal basis	Art 88 II GDPR i.c.w. WCA 365, Art 88 II GDPR i.c.w. WCA Exchange, Art. 6 I d GDPR, Art. 6 I f GDPR legitimate interest, whereas the legitimate interest is to sort and access business communication, defend ourselves in case of legal disputes and ensure compliant and legal behavior of users, defend , Art 88 I GDPR i.c.w. Art 26 II Bundesdatenschutzgesetz (“BDSG”) for investigation against employees. There may be additional legal basis based on the reason for the search.

Please note that there are additional connected services that Microsoft offers, in which case, Microsoft processes Personal Data as independent controller, such as Weather or Translate. Using these services transfers the Personal Data out of Exyte’s control to Microsoft’s control based on your instruction. You will find the information about Microsoft processing personal data as controller under this link:

Microsoft Privacy Statement – Microsoft privacy

6. EHS App

In the frame of the EHS App or the website we process personal data for Safe Behavior Observations and 2 Person High Risk Inspection.

These functions process the personal data as described above.

In regard to the content of the data you enter, we generally process the following information:

- Name
- Employer
- Construction Site
- Reporting Date
- Reporting Details
- Remedy Measures
- Photos

You may also be subject to such report. Generally the report itself and attached photos should not contain personal data, but only company data. In some cases persons might be identified coincidentally or through deduction.

We process such Personal Data in order to improve and maintain safety on our construction sites.

Processing is based on Art. 6 Sect I Lit. f GDPR, whereas it is our legitimate interest to keep everyone on the construction sites safe.

Safe behavior observations are deleted or anonymized after 6 months.

Two person high risk inspections are kept for the duration of a project or, if a risk manifested, until the consequences are resolved (e.g. compensation for injured persons).

If the Personal Data become part of an official report, they may be stored for the retention time of the report, depending on local laws and regulations. We may provide you with additional information, where required.

7. Source of the Personal Data

Personal Data we receive are either Personal Data you enter into the platform or you send to the M365 System or the M365 System collects such data about you, while you are working on the M365 platform. Also third parties may enter Data about you in the system.

8. Transfer

We may transfer Personal Data between Exyte affiliates within the Exyte Group based on our legitimate interest according to Art. 6 para. I lit. f GDPR, whereas our legitimate interest is to organize the company group centrally and provide services within group service centers as well as to have the processing allocated at the most suitable group member for further interaction with the data subject.

All group members are subject to a Data Protection Policy to ensure a constant level of data protection.

Some Exyte Group members may be located outsider the European Economic Area (“EEA”) in countries for which the European Commission (“EC”) did not decide that such countries provide an adequate level of data protection.

All Exyte Group members therefore signed a Data Processing and Joint Controller Agreement (“DPJCA”) which includes the standard contractual clauses as approved by the EC to safeguard the processing of Personal Data outside the EEA, i.e. all Exyte Group members are contractually obligated to comply with an adequate data protection level.

Please find a list of all Exyte entities belonging to the Exyte Group under this link.

We may further transfer Personal Data to service providers which provide services to us. We concluded agreements with such service providers about the use of Personal Data they process for us based on our instructions.

In the frame of support and processing activities by Microsoft, whereas Exyte content data shall remain in Europe, diagnostic data and other generated data in the frame of processing according personal data may be processed by Microsoft affiliates worldwide (also depending on your location). We concluded a data processing agreement including safeguards with Microsoft in order to protect your personal data.

Especially in the frame of security issues and login data from your user profile, such as time and location may be transferred to Microsoft affiliates, also outside the EEA. This is e.g. to identify coordinated hacker attacks or to identify suspicious behavior (e.g. if the same user suddenly logs in from an impossible location or if several users log in coordinated from the same location across different organizations. According to Microsoft, such Personal Data are pseudonymized on-site of the tenant and Microsoft does not have the ability to de-pseudonymize the Personal Data.

Where such transfer becomes necessary, we concluded the Standard Contractual Clauses as approved by the European Commission. Furthermore, the Microsoft cooperation is certified under the EU-US Data Privacy Frame Work, resulting being subject to an Adequacy Decision by the European Commission.

Besides the transfer within the Exyte Group and in the frame of processing by Microsoft a transfer of Personal Data to third parties does not take place, with the exception of:

- Transfer with your express permission (Art 6 para. I lit a GDPR or Art 9 para I GDPR);
- Transfers to third parties that we engage to fulfill contractual and delivery conditions, such as banking institutions that process payments, subcontractors, as well as transportation companies / shipping companies handling deliveries based on Art 6 para I lit b GDPR if the data subject is the contract partner otherwise based on Art 6 para I lit f GDPR with the legitimate interest to initiate, settle and implement the contract;
- Transfer to third parties Exyte engages in marketing and advertising for our own products and services, such as printing agencies according to Art. 6 para. I lit. f GDPR. Our legitimate interest to process your data stems from our desire to promote, sell, and improve our own products and services;
- Transfers to third parties to which we are legally obliged, for example to the tax office or other governmental authorities, according to Art. 6 para I c GDPR;
- Transfers to third parties to fulfill our commercial and tax obligations, for example to our tax auditor according to Art. 6 para I c GDPR i.c.m with the respective individual obligation, if we are legally obliged to transfer such data or Article 6 para I f GDPR, if the transfer is not mandatory, but required for our legitimate interest to efficiently communicate and proceed with authorities and comply with our obligations; Even if not required by law, we may decide to cooperate with authorities and provide personal data in the course of an investigation based on This based on our legitimate interest to avoid legal escalation or in accordance with § 23 and 24 Bundesdatenschutzgesetz

(BDSG) or our legitimate interests to support authorities in their legal tasks and avoid a legal escalation in accordance with Art 6 Sect I Lit. f GDPR.

- We may provide personal data from our M365 System to client or sub-contractors to comply with contractual agreement, assert or defend from legal claims, track progress or provide other services (e.g. to track changes on a construction document within DMCS). This is based on our legitimate interest to provide services to our client, organize our services efficiently and assert or defend from claims in accordance with Art 6 Sect I Lit f GDPR.
- In order to assert legal claims or to defend against legal claims, we may transfer data to authorities or to lawyers, agents, experts etc. based on Art. 6 para I lit f GDPR, whereas it is our legitimate interest to assert or defend from legal claims. In case of special categories of Personal Data, we may transfer such data based on Art. 9 para II lit f GDPR to assert or defend against a legal claim.
- In order to support an authority investigation we may provide information to authorities base on Art. 6 Sect I lit f GDPR, whereas it is our legitimate interest to support legitimate authority investigations, where permitted by the GDPR. Where required to cooperate by law, we will provide such information based on the respective law.

Please contact us if you require more information.

9. Duration of processing

We will process your Personal Data only for the period (time) which is necessary to complete the purpose.

If you provided us with your consent, we will process your data until you recalled such consent.

For content data, the retention of data will depend on the content and we will inform you separately where necessary.

E.g. for projects and due to warranty and guarantee obligations the processing periods are usually as follows:

- If you are engaged in a project, up to 12 years from completion of the project in order to fulfil and comply with quality control and guarantee obligations, whereas this storage can be extended in case of lawsuits or authority audit;
- If your Personal Data are included in commercial communication and documents, we may store your data up to 10 years to comply with documentation duties, such as Art. 257 ff. Handelsgesetzbuch or Art 147 Abgaben Ordnung;

Otherwise as part of keeping our system secure, M365 log files are kept for 1 year, unless we identify a risk, incompliance, or criminal activities or infringements of applicable regulations or the code of conduct.

If feasible based on the applicable law or our legitimate interests, we will delete your Personal Data earlier.

We may, however, have to retain your Personal Data for longer in case of legal obligations (e.g. a tax audit) or to defend from or assert a legal dispute or during an investigation of a breach of laws or regulations or our code of conduct or other authority investigations.

Furthermore, we may store your contact data as long as there is a legitimate interest to remain in contact with you based on our last communication or contact with you.

10. Recording or transcription of Teams meetings or calls

Microsoft Teams has the function of recording or transcription (following referred to as “Recording”) of meetings. Live transcription or translation for easier understanding, which is not recorded or stored longer than the meeting does not fall under Recording. You will find more information about this below.

Generally, as good practice at Exyte recommends not to Record meetings; however, in some cases, recording may e.g. be necessary for future review, creation of meeting minutes, or to ensure that all required and interested parties can access pertinent information covered during the course of the meeting.

Additional exceptions may exist where Exyte has a legitimate interest to record Teams meetings.

To safeguard your interests, when the recording is switched on your camera and microphone are switched of and you are asked to give your consent to the recording by switching them on again. A po-up within the Teams meeting (which provides additional detaills) will alert you, the meeting participant..

By activating your camera or microphone upon being requested you consent to the recording of your image and/or voice (Art 6 Sect I a GDPR, Art 9 Sect II a) GDPR).

Should the consent not be valid or applicable, we process your image and your voice based on our legitimate interest (Art 6 Sect I Lit f) GDPR, whereas it is our legitimate interest to effectively organize our business and our employee´s time, in particular to effectively organize meetings and trainings and reach as many interested parties as possible.

The purpose is to provide people, which are not present at a Teams meeting, with access to the specific meeting content or training or to enable participants the opportunity to revisit the content later and to effectively organize Exyte and the time of the employees as well as to provide flexibility.

Unless you are informed otherwise, Recordings are automatically deleted after 60 days.

If your processing is based on your consent, you can revoke that consent at any time and we will stop processing. When processing is based on our legitimate interest, we extend the same option to you, unless you have been informed specifically otherwise, e.g. because we have a contractual obligation to record a meeting.

Revocation of your consent does not effect processing before revocation.

Live / real time transcriptions and translations are based on Art 6 Sect I Lit f GDPR, whereas it is our legitimate interest to make meetings accessible to as many as possible persons no matter how good they are in the spoken language or whether they have an impairment.

The purpose is to enable participants to follow the call more easily.

Life / real time transcriptions or translations are deleted latest at the end of the call and only stored for technical reasons beyond being shown on the screen.

11. NO AUTOMATED DECISION MAKING

We do not base decisions which produce legal or similar significant affects to you solely on automated decision making, such as profiling.

However, security screening (e.g. abnormal behavior) may be automated and based on your general behavioral profile in the M365 platform. Being wrongly flagged as potential security threat will have no significant negative impact on you, as there will always be a team at Exyte, which will investigate the flag.

12. YOUR RIGHTS

Upon request we will inform you whether Exyte processes any Personal Data about you, and if yes which.

If we process your Personal Data in order to advertise, you have the right to object to the processing of your Personal Data for the purpose of advertising at any time. If you object to the processing for purposes of advertising, your Personal Data will no longer be processed for this purpose.

The easiest method to object to advertisement is to send an email to info@exyte.net. However, we accept any other form of objections to advertisement, which allows us to clearly identify you.

Furthermore, you have the right to object against processing of your Personal Data, based on your particular situation, in case of processing which is processed based on Article 6 para. I lit. f GDPR, i.e. legitimate interest, or Art 6 para. I lit e GDPR, i.e. processing based on necessity for the performance of a task carried out in the public interest or in the exercise of official authority vested in Exyte including if we use your personal data for profiling for that purpose. In case you object to processing based on the aforementioned legal basis due to your particular situation, we will only proceed processing, if our compelling legitimate grounds to process your data overrides your interest, rights or freedoms to stop processing your Personal Data or for the exercise or defense of legal claims. This also applies to profiling based on the aforementioned.

Under the conditions as set out in the GDPR, according to Art. 16 GDPR you also have the right to correct your incorrect or incomplete Personal Data as well as a right to deletion according to Art. 17 GDPR and a right to restrict the processing of your Personal Data under Art. 18 GDPR.

You also have the right to receive from us Personal Data concerning you, which you have provided to us, in a structured, commonly used, and machine-readable format. You have the right to transmit (or have transmitted) the Personal Data to another controller (Art 20 GDPR).

If the processing of Personal Data concerning you is based on your consent, you have the right to revoke your consent at any time. The lawfulness of the processing on the basis of the consent until the revocation is not affected.

You also have the right to lodge a complaint with the competent supervisory authority for data protection matters. Unless stated otherwise, the competent authority is the “Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg” in Baden-Württemberg, Germany.

You can always lodge a complaint at the data protection officer or commissioner at the location of the Exyte Group entity within the EEA you or the Business Partner is working for has a contract with.