Data Protection Information
on our processing of employee data pursuant to Art. 13, 14 and 21 GDPR
Version 5.1 – As of: 02.10.2026

CONFIDENTIAL
This document contains confidential information.
If you are not the intended recipient, please inform the sender and delete this document. Any unauthorised reproduction, disclosure or distribution of the material is strictly prohibited.

Data Protection Information for Employees

CSP Intelligence GmbH
Herrenäckerstraße 11
94431 Großköllnbach

Dear Employee,

In accordance with the requirements of Art. 13, 14 and 21 of the General Data Protection Regulation (GDPR), this information sheet informs you about the processing of the personal data collected from you as well as your associated data protection rights. To ensure that you are fully informed about the processing of your personal data in connection with the establishment, performance and termination of the employment relationship, please take note of the following information.

Data Protection Information

on our processing of employee data pursuant to Art. 13, 14 and 21 GDPR

Version 5.1 – As of: 02.10.2026

CONFIDENTIAL

1. Controller within the meaning of data protection law

CSP Intelligence GmbH
Herrenäckerstraße 11
94431 Großköllnbach
Phone: 09953 3006-0
info@csp-sw.de
www.csp-sw.de

2. Contact details of our Data Protection Officer

Kemal Webersohn, LL.M.
WS Datenschutz GmbH
Dircksenstraße 51
10178 Berlin
Email: csp@ws-datenschutz.de

3. Purposes and legal basis of the processing

We process your personal data in accordance with the provisions of the European General Data Protection Regulation (GDPR) and the German Federal Data Protection Act (BDSG), insofar as this is necessary for the employment relationship. The legal basis for this is Art. 88 GDPR in conjunction with Sec. 26 BDSG as well as, where applicable, Art. 6 (1) (b) GDPR for the initiation or performance of contractual relationships.

Furthermore, we may process personal data about you insofar as this is necessary to defend against asserted legal claims arising from the employment relationship against us. The legal basis for this is Art. 6 (1) (f) GDPR, the legitimate interest being, for example, a duty to provide evidence in the context of legal proceedings. Insofar as you grant us your express consent to the processing of personal data for specific purposes, the lawfulness of this processing is based on your consent pursuant to Art. 6 (1) (a) GDPR. Any consent given may be withdrawn at any time (see section 9 of this data protection information). Please note that the withdrawal only takes effect for the future. Processing operations carried out prior to the withdrawal are not affected.

In accordance with Art. 88 GDPR in conjunction with Sec. 26 BDSG, we may further process the personal data already obtained from you in the course of an application procedure for

purposes of the employment relationship, insofar as this is necessary for the commencement, performance or termination of the employment relationship or for the exercise or fulfilment of the rights and obligations of the employees' representative body arising from a law or a collective bargaining agreement, a works or service agreement (collective agreement).

Security awareness training and phishing simulations with SoSafe

To train our employees and to protect our IT systems, we use the platform of SoSafe SE, Lichtstraße 25a, 50825 Cologne, Germany. Via SoSafe, information security training and simulated phishing attacks are carried out. In this context, in particular name, business email address, learning progress and reactions to simulated phishing emails are processed. This includes, for example, opening emails, clicks, replies, learning tips read and reported emails.

The legal basis for the processing is Sec. 26 (1) BDSG in conjunction with Art. 88 GDPR as well as Art. 6 (1) (f) GDPR. Our legitimate interest lies in protecting our IT systems, personal data and trade secrets and in preventing security incidents.

The results of the phishing simulations can be attributed to individual employees. Access to them is restricted exclusively to four persons authorised for this purpose. The evaluation serves to improve information security and to identify any need for training. The results are not used for general performance or behavioural monitoring or for automated decisions under employment law. The results are stored for the duration of the respective campaign, for a maximum of one year.

For individual technical services, SoSafe uses the sub-processors Amplitude, Inc. and Zendesk, Inc., each based in the USA. Amplitude processes pseudonymised user and device IDs as well as clicks on the learning platform, the manager platform and the phishing report button. The actual IP addresses are protected by a privacy proxy and are not visible to Amplitude. The pseudonymised usage data is currently stored for the duration of the contractual relationship with SoSafe and anonymised thereafter. In the context of support requests, Zendesk processes in particular name, business email address, user role, customer assignment and the content of the submitted tickets.

The data is generally stored in the European Union. In individual cases, authorised employees of the sub-processors may access the data from the USA for support, maintenance or troubleshooting purposes. The transfer is based in particular on the EU-U.S. Data Privacy Framework and, additionally, on the Standard Contractual Clauses of the European Commission. Further information on data processing can be found at https://sosafe-awareness.com/privacy-policy/.

Data Protection Information

on our processing of employee data pursuant to Art. 13, 14 and 21 GDPR

Version 5.1 – As of: 02.10.2026

CONFIDENTIAL

Pleo

We use the platform "Pleo" (Pleo Technologies, Ravnsborg Tværgade 5C, 2200 Copenhagen, Denmark) to manage business expenses, company cards, receipts, reimbursements and the related accounting and settlement processes. In doing so, we process personal data of our employees insofar as this is necessary for the provision and use of the platform, the management of business expenses, the recording and review of receipts, the processing of card transactions, the handling of reimbursements, technical operation and support.

We process this data to perform the employment relationship, to properly settle business expenses, to comply with commercial and tax documentation obligations, and to safeguard our legitimate interests in efficient, secure and traceable expense management. The legal bases are, in particular, Art. 6 (1) (b) GDPR in conjunction with Sec. 26 BDSG insofar as the processing is necessary for the performance of the employment relationship, Art. 6 (1) (c) GDPR insofar as statutory retention, evidence or accounting obligations exist, and Art. 6 (1) (f) GDPR insofar as the processing is necessary for the secure, efficient and abuse-preventing management of business expenses.

Pleo processes personal data in connection with the provision of the platform generally as a processor pursuant to Art. 28 GDPR on the basis of a data processing agreement and thus on our instructions. According to the contractual classification, Pleo does not use personal data for its own purposes, in particular for product improvement, analytics, benchmarking, profiling or AI/model training, on the basis of personal customer data; insofar as Pleo uses data for statistical analysis, system optimisation or service improvement, this is done only in aggregated or anonymised form. Independently of this, Pleo may act as an independent controller in certain areas, in particular for processing carried out to fulfil its own legal or regulatory obligations as a financial service provider (such as identity checks, KYC/AML checks, sanctions-list screening, fraud prevention, payment and card processes, and statutory retention obligations). The use of Pleo does not serve the purpose of covert performance or behaviour monitoring of our employees.

Perk

We use the platform Perk to organise business trips, manage travel bookings and settle travel expenses and reimbursements. The AI function of Perk is currently not used.

The processing is carried out to organise, perform and settle business trips, to manage travel costs and expenses, for the internal approval and control of expense-relevant transactions, and to comply with statutory evidence, tax and retention obligations. The legal bases for the processing are Art. 6 (1) (b) GDPR or Sec. 26 BDSG insofar as the processing is necessary for the performance of the employment relationship, Art. 6 (1) (c) GDPR insofar as statutory obligations are fulfilled, and Art. 6 (1) (f) GDPR insofar as there are legitimate interests in efficient travel organisation, settlement, abuse prevention, IT security and administration.

Perk processes personal data on our behalf on the basis of a data processing agreement pursuant to Art. 28 GDPR. Perk is used exclusively for business purposes; it is not used for performance or behaviour monitoring.

Exa Web Search

We use the AI-assisted web research tool "Exa Web Search" (Exa Labs Inc., 430 Shotwell Street, San Francisco, CA 94110, USA) for internal market and competitive intelligence. Login is performed using your business email address.

In this context, we process your data to provide and administer the tool, to ensure IT security and to enable proper and traceable use. The legal basis is Art. 6(1)(f) GDPR (legitimate interest in the secure and proper operation of the tool) and Section 26(1) BDSG in the employment context.

Exa processes personal data on our behalf on the basis of a data processing agreement pursuant to Art. 28 GDPR.

4. Categories of personal data

We process data that is connected with your employment relationship. This may include general data relating to your person (such as name, address and contact details), information on your professional qualifications and schooling or information on professional development, as well as data serving the fulfilment of contractual obligations and accounting and tax obligations (bank details, health insurance, social security and tax data, etc.), participation and completion data for internal training courses, and click behaviour in simulated phishing emails.

In connection with the use of Pleo (see section 3), we process in particular the following categories of personal data:

- Master and contact data, in particular name, business email address, telephone number, position/function, user name and organisational assignment
- Employment-related data, in particular employer, activity, area of responsibility and, where applicable, location details
- Financial and transaction data, in particular bank account details, payment information, purchase, card and expense history
- Receipt data, in particular invoices, receipts, merchant details, amounts, posting texts, cost centres, purposes of use and uploaded supporting documents
- Technical usage and security data, in particular IP address, login data, device information and log data

Insofar as Pleo carries out independent checks as a financial service provider (e.g. identity, KYC/AML and sanctions-list checks), for regular users in particular name, business email address and information on the country of residence or nationality may be processed; for legal representatives, beneficial owners, administrators or other persons subject to verification, additionally date of birth, identity-document data and proof of identity, insofar as this is legally required.

We ask you to upload only such receipts and information when using Pleo as are necessary for the settlement of business expenses. Private or unnecessary information should, where possible, be avoided or redacted, in particular where receipts could allow conclusions to be drawn about specially protected information (such as health data, religious or political references or comparable sensitive matters).

In connection with the use of Perk (see section 3), the following categories of personal data may be processed in particular:

- Name, business contact details, telephone number, business address, job title and role assignment
- User and access data within the platform
- Data for planning and carrying out business trips, in particular travel destinations, travel times, travel histories, booking data for hotels, flights, train journeys or rental cars
- Information on loyalty programmes, insofar as this is provided voluntarily
- Settlement-relevant data, in particular invoice information, expense details, receipts and payment information
- Restricted credit card data, e.g. card type, last four digits and expiry date
- Location data for mileage calculation, insofar as this function is used; no real-time tracking takes place in this context

- Communication content in connection with support requests

Employees are asked not to enter any sensitive or unnecessary personal data in free-text fields and support requests, and to upload receipts only to the extent necessary.

In connection with the use of Exa Web Search (see section 3), we process in particular the following categories of personal data:

- Account and contact data, in particular name and business email address
- Technical usage and security data, in particular IP address, login/log data and the time and extent of use

Please do not enter any personal data into search queries and do not conduct targeted research on individuals (see internal usage policy).

5. Sources of the data

We process the personal data that you have provided for the purpose of establishing and performing the employment relationship. This includes data that you provide to us directly (e.g. in the application process, for the personnel file), as well as data that arises in the course of your work or through the use of our IT systems (e.g. click behaviour in phishing simulations, access data). In addition, we may have lawfully obtained data from publicly accessible sources (e.g. EU terrorist lists, UN sanctions lists) or third parties (e.g. authorities, former employers with your consent).

6. Recipients of the data

Within our company, we pass on your personal data exclusively to those departments that require this data to fulfil the contractual and statutory obligations or to implement our legitimate interest.

We may transfer your personal data to companies affiliated with us, insofar as this is permissible within the scope of the purposes and legal bases set out in section 3 of this data protection information.

Otherwise, data is only passed on to recipients outside the company insofar as statutory provisions permit or require this, the disclosure is necessary for processing and thus for the fulfilment of the employment contract, you have consented, or we are authorised to provide information. Under these conditions, recipients of personal data may be, for example:

- Public bodies and institutions (e.g. the tax office) where there is a statutory or official obligation.
- Recipients to whom the disclosure is directly necessary for the establishment or performance of the contract, such as authorities, insurers, financial service providers, hotels, transport service providers, customers.
- Further data recipients may be those bodies for which you have granted us your consent to transfer the data.

In connection with the use of Pleo (see section 3), personal data may be transferred within the Pleo group as well as to service providers, sub-processors, payment service providers, card providers, banks, technical service providers, support service providers, advisers or authorities engaged by Pleo, insofar as this is necessary for the aforementioned purposes or required by law. Internally, we restrict access to expense, receipt and transaction data to the persons responsible and authorised for this purpose, in particular accounting, authorised managers, administration and, where applicable, data protection or compliance functions.

In connection with the use of Perk (see section 3), depending on the trip booked or the function used, data may be transferred to travel providers, payment service providers, hotels, airlines, rental-car providers, rail companies or other recipients necessary for handling the trip. Depending on the constellation, these recipients may be independent controllers.

In the Perk Travel module, according to Perk's own information, Perk uses OpenAI for data analysis and classification, in particular in connection with travel disruptions, notifications and

the assessment of travel-related processes. According to Perk, names, email addresses, travel histories and free-text fields in particular may be processed in this context. Perk states that personal customer data is not used to train or improve third-party AI models and that no human review by OpenAI takes place. According to Perk, expense receipts, invoice content, screenshots, identity documents and A1 or social security data are not transferred to OpenAI.

In connection with the use of Exa Web Search (see section 3), personal data is passed on to the provider Exa Labs Inc. and its subcontractors (in particular cloud and infrastructure providers), insofar as this is necessary for the provision of the service.

7. Transfer to a third country

Your personal data is generally stored and processed in data centres within the European Union. Access may be required in particular for technical support, system maintenance or troubleshooting. The transfer of personal data to the USA takes place on the basis of the adequacy decision of the European Commission pursuant to Art. 45 GDPR. In addition, the Standard Contractual Clauses of the European Commission pursuant to Art. 46 (2) (c) GDPR may be agreed.

In connection with the use of Pleo (see section 3), processing may take place outside the European Union or the European Economic Area in individual cases. In such cases, appropriate safeguards pursuant to Chapter V GDPR are used, in particular adequacy decisions, standard contractual clauses and supplementary risk assessments.

In connection with the use of Perk (see section 3), processing of personal data may also take place outside the European Union or the European Economic Area. Perk states that it uses appropriate safeguards for this purpose, in particular EU standard contractual clauses, transfer impact assessments and supplementary technical, organisational and contractual protective measures.

In connection with the use of Exa Web Search (see section 3), personal data is also processed in the USA. The transfer is safeguarded by EU Standard Contractual Clauses; a transfer impact assessment is available.

8. Duration of data storage

We process your personal data for as long as this is necessary for the establishment, performance or processing of the employment relationship or for the exercise or fulfilment of the rights and obligations arising from the employment contract, or for the exercise or fulfilment of the rights and obligations of the employees' representative body arising from a law or a collective bargaining agreement, a works or service agreement (collective agreement).

In addition, we are subject to various retention and documentation obligations arising, among other things, from the German Commercial Code (HGB) and the German Fiscal Code (AO). The retention or documentation periods stipulated therein range from two to ten years.

Finally, the storage period is also determined by the statutory limitation periods which, for example pursuant to Sec. 195 et seq. of the German Civil Code (BGB), are generally three years but in certain cases may be up to thirty years.

For the data processed via Pleo (see section 3), the following applies: we store personal data only for as long as is necessary for the respective purposes. Insofar as commercial, tax, anti-money-laundering, payment-services or other statutory retention obligations exist, individual data may continue to be stored even after the end of use or of the employment relationship.

In connection with the use of Perk (see section 3), personal data is stored only for as long as is necessary for the stated purposes or as long as statutory retention and evidence obligations exist. After the purposes cease to apply or the statutory retention periods expire, the data is deleted or anonymised.

In connection with the use of Exa Web Search (see section 3), account and usage data is stored only for as long as is necessary for the operation of the tool, at most until the end of use plus any statutory retention periods. Search queries are deleted immediately after they are answered where the "Zero Data Retention" function is activated.

9. Your rights

Every data subject has the right of access pursuant to Art. 15 GDPR, the right to rectification pursuant to Art. 16 GDPR, the right to erasure pursuant to Art. 17 GDPR, the right to restriction of processing pursuant to Art. 18 GDPR, the right to notification pursuant to Art. 19 GDPR, and the right to data portability pursuant to Art. 20 GDPR.

In addition, you have the right to lodge a complaint with a data protection supervisory authority pursuant to Art. 77 GDPR if you are of the opinion that the processing of your personal data is not lawful. The right to lodge a complaint exists without prejudice to any other administrative or judicial remedy. The supervisory authority responsible for us is:

Bavarian State Office for Data Protection Supervision (Bayerisches Landesamt für Datenschutzaufsicht)
Michael Will, President of the Bavarian State Office
Promenade 18
91522 Ansbach
https://www.lda.bayern.de/de/index.html

Insofar as the processing of data is based on consent given by you, you are entitled pursuant to Art. 7 GDPR to withdraw your consent to the use of your personal data at any time with effect for the future. Please note that we may have to retain certain data for a specific period in order to comply with statutory requirements (section 8 of this data protection information).

Right to object

Insofar as the processing of personal data concerning you is carried out on the basis of Art. 6 (1) (f) GDPR to safeguard legitimate interests, you have the right to object at any time, on grounds relating to your particular situation, to the processing of this data pursuant to Art. 21 GDPR. We will then no longer process this personal data unless we can demonstrate compelling legitimate grounds for the processing which override your interests, rights and freedoms, or the processing serves to assert, exercise or defend legal claims.

Insofar as Pleo acts as an independent controller in connection with the use of the platform (see section 3), you may additionally exercise the aforementioned rights directly vis-à-vis Pleo. Further information on data processing by Pleo can be found at https://www.pleo.io/legal-documents/pleo-privacy-policy-de.pdf.

In connection with the use of Perk (see section 3), Perk processes your data as a processor; insofar as individual travel providers (e.g. hotels, airlines) are independent controllers depending on the booking, you may additionally exercise your rights directly vis-à-vis them. Further information on data processing by Perk can be found at https://www.perk.com/legal/privacy-policy/.

In connection with the use of Exa Web Search (see section 3), Exa processes your data as a processor. Further information on data processing by Exa can be found at https://exa.ai/privacy-policy.

To safeguard your rights, you may contact us at any time using the details given above.

10. Necessity of providing personal data

The provision of personal data in connection with the conclusion of an employment relationship is neither required by law nor by contract. You are therefore not obliged to provide the personal data. However, the provision of personal data is necessary for the conclusion of the employment relationship (employment contract) with us. In connection with the conclusion of the employment relationship, however, you should only provide such personal data as is necessary for the commencement and performance of the employment relationship. Insofar as you do not provide us with any personal data upon conclusion of the employment relationship, we cannot conclude an effective employment relationship with you.

11. Anti-Terrorism Regulations

In accordance with the European anti-terrorism Regulations (EC) No. 2580/2001 and No. 881/2002, we verify, within the scope of statutory obligations, that no financial or economic resources are made available to listed persons or organisations, in order to prevent the financing of terrorist activities.
For this purpose, personal data such as the names and dates of birth of applicants, employees and temporary workers may be checked against sanctions lists such as the EU terrorist lists and UN sanctions lists . This check is carried out regularly as well as when new employees are hired

and is based on Article 6 (1) (c) GDPR. Data is only passed on to the competent authorities to the extent necessary.

12. Automated decision-making

We do not make any automated decisions in individual cases within the meaning of Art. 22 GDPR with regard to decisions concerning your employment relationship.