LOGENT
SUPPORTING LOGISTICS

2024

Privacy Policy (GDPR)

Administered by: HR Department
Approved by: CEO Logent Group
Valid from: 2024-02-06
Valid until: Until further notice

LOGENT
SUPPORTING LOGISTICS

1. Purpose and scope

This privacy policy explains how Logent processes personal data about you as an employee (including former employees), consultant/temporary staff and job applicant in connection with recruitment, employment and related processes. This policy is an information notice under the GDPR and is supplemented by internal governing documents and procedures (e.g. retention schedule, information security procedures, access management and the CCTV Policy where camera surveillance is used).

2. Controller, contact details and Data Protection Officer (DPO)

The company within the Logent group that is your employer (or that is responsible for the relevant recruitment process) is the controller for the processing. In some cases, group-wide functions or several companies may be joint controllers (e.g. for shared IT/HR processes). Upon request, you can receive more information about which company is responsible in a specific case.

Contact for data protection matters: it@logent.se

Postal address: Hammarby Kaj 14, 120 30 Stockholm – Attention GDPR.

Data Protection Officer (DPO): Logent has currently not appointed a Data Protection Officer. Data protection matters are handled via the contact details above.

3. Which personal data we process

Depending on your role and situation, we may process the following categories of personal data:

- Identity and contact data (e.g. name, national ID number, address, phone number, email).
- Employment and assignment data (e.g. job title, type of employment/assignment, start/end date, organisational unit).
- Salary and benefits data (e.g. salary, allowances, benefits, bank details, tax data).
- Time and absence data (e.g. schedule, time reporting, leave, absence codes to the extent required).
- Work environment/rehabilitation (limited health data where required by law/agreements, e.g. certificates and rehabilitation measures).
- IT and security data (e.g. access rights, access logs, device information, incident data).
- Business communications (e.g. email, Teams, case handling, to the extent needed for work).
- Data in connection with investigations, incidents and disputes (e.g. employment law matters, disciplinary measures).
- Recruitment data (e.g. CV, application, interview notes, references).
- Image/video/audio (e.g. photo for access card or intranet; where applicable communications/marketing).
- CCTV footage (where camera surveillance is used in the business).

4. Where does the data come from?

We process personal data only when we have a clear purpose and a lawful basis under the GDPR. The most common sources are:

- You (e.g. when you apply for a job, during onboarding, in HR/self-service systems).
- Your manager/HR and other internal functions (e.g. for scheduling, payroll, access administration).
- External parties where relevant and permitted (e.g. authorities, benefit providers, occupational health services, references in recruitment).
- Systems and logs generated through the use of IT systems, access systems and security solutions.

5. Why we process personal data and lawful basis

We process personal data only when we have a clear purpose and a lawful basis under the GDPR. The most common lawful bases in an employment context are:

- Contract – processing is necessary to perform the employment contract or to take steps prior to entering into a contract.
- Legal obligation – e.g. tax, accounting, work environment and employment law requirements.
- Legitimate interests – e.g. access administration, IT security, internal communication, operational and quality follow-up, and to establish, exercise or defend legal claims.
- Consent – used restrictively in working life and only where consent can be genuinely voluntary and can be withdrawn without negative consequences.

Examples of common processing activities (overview):

Purpose	**Examples**	**Lawful basis (typical)**	**Retention (principle)**
Employment and payroll administration	Salary, allowances, taxes, pension and benefits administration, reporting.	Contract / Legal obligation	During employment and thereafter as required by law and the retention schedule (e.g. accounting).
Time reporting and staffing	Scheduling, time bank, absence, planning, staffing follow-up.	Contract / Legal obligation / Legitimate interests	According to collective agreements/law and the retention schedule.
Access rights, IT and security	Access provisioning, logs, device management, incident management.	Legitimate interests / Legal obligation	As long as needed for security and follow-up according to the retention schedule.
Work environment and rehabilitation	Work environment measures, rehabilitation plan, occupational injury, contact with occupational health services.	Legal obligation / (special categories, see section below)	Limited retention according to legal requirements and retention schedule; strict access controls.
Recruitment	Selection, interviews, references, background checks where justified.	Legitimate interests / Contract (pre-employment)	Limited time after completion according to

			recruitment procedure.
Investigations, incidents and disputes	Investigation of incidents, disciplinary matters, whistleblowing (if applicable), disputes.	Legitimate interests / Legal obligation	As long as the case is ongoing and thereafter with regard to limitation periods and the retention schedule.
Internal communication and organisational information	Contact lists, intranet, internal news, organisational data.	Legitimate interests	During employment and thereafter for a short period according to the retention schedule.

6. Special categories of personal data (e.g. health)

Certain personal data is particularly sensitive ("special categories"), such as health data. Such data is processed only when necessary and lawful, for example to meet obligations in employment and work environment law, handle rehabilitation or occupational injuries. Access to such data is strictly limited (need-to-know) and protected by enhanced security measures.

7. Whether you must provide data and consequences

Some data is needed to enter into and perform an employment contract (e.g. contact details and bank details), and other data is needed to comply with legal obligations (e.g. national ID number and data required for tax and work environment reporting). If you do not provide necessary data, this may mean that we cannot administer your employment, pay salary, or grant access to systems and the workplace.

8. Recipients, processors and disclosures

We may share personal data with:

- Processors that process data on our behalf (e.g. HR/payroll systems, time reporting systems, IT operations, recruitment systems, occupational health services).
- Independent controllers (e.g. authorities, banks, insurance companies, pension providers).
- Group companies and group-wide functions where required for administration, security or compliance.

When we engage processors, we enter into data processing agreements and require security, confidentiality and controls regarding sub-processors. Disclosures to third parties take place only when there is a lawful basis, e.g. a legal obligation or legitimate interests (for example in investigations of crime or incidents).

9. Transfers outside the EU/EEA

If personal data is transferred to countries outside the EU/EEA (e.g. through cloud services or group-wide IT), we ensure that the transfer has a lawful basis, for example through the European Commission's Standard Contractual Clauses (SCC) a nd supplementary safeguards where required (e.g. a transfer impact assessment (TIA)).

10. Retention and deletion

We keep personal data as long as it is needed for the purposes and in accordance with applicable legal requirements. Thereafter, data is deleted or anonymised in line with Logent's retention schedule. Different data types have different retention requirements. Examples:

- Documentation subject to accounting rules may need to be retained for several years (under applicable law).
- Data in dispute and investigation cases is retained as long as justified with regard to the nature of the case and limitation periods.
- IT security logs are normally retained for a limited period and in accordance with security and incident procedures.

Detailed retention periods are set out in Logent's retention schedule: *M:\Verksamhetssystem\12. Chefshandbok - NY (uppdateras löpande)\11. GDPR – Personaldokument*.

11. Automated decision-making and profiling

Logent does not use automated decision-making that produces legal effects concerning you, or similarly significantly affects you, based solely on automated processing, unless otherwise stated in specific information for a particular process (e.g. recruitment). If such processing were to occur, we will provide specific information, including the logic involved and your rights.

12. CCTV (camera surveillance)

In some operations, Logent may use camera surveillance for security and safety purposes, for example to prevent, detect or investigate crime or serious incidents. Camera surveillance is never used for the purpose of routinely monitoring employees' work performance.

From 1 April 2025, new rules apply to camera surveillance. In summary:

- No one needs to apply to IMY for a permit to conduct camera surveillance.
- Actors that previously required a permit must carry out their own balancing test between the surveillance interest and the individual's interest in not being monitored.
- The balancing test must be documented. Logent also documents assessments as part of GDPR accountability.
- Where required, the party conducting camera surveillance must also keep a record with certain information about the surveillance carried out, or that has ceased within the last five years. As part of GDPR accountability, Logent documents and retains information about ceased camera surveillance in the record for up to five years.

Camera surveillance is regulated in more detail in Logent's CCTV Policy, which, among other things, describes placement, signage and supplementary information, retention periods, access and logging, disclosures (e.g. to law enforcement authorities), incident handling and templates for the balancing test and record. The policy also states that surveillance must not take place in areas where the privacy intrusion is normally particularly significant (e.g. changing rooms and break areas) and that audio recording is normally not used.

Requests for access to CCTV footage are handled via Logent's data protection contact. Logent may need to verify identity and narrow the request (e.g. time and location). Where footage includes other individuals, their privacy is protected through measures such as masking/redaction or limiting

disclosure. In complex cases or where there is uncertainty, the matter is escalated to the Legal/DPO function in accordance with internal procedures.

13. Your rights

Depending on the circumstances, you have the following rights:

- Right to information and access (data subject access request).
- Right to rectification of inaccurate data.
- Right to erasure in certain cases.
- Right to object to processing based on legitimate interests.
- Right to restriction of processing in certain cases.
- Right to data portability where processing is based on contract or consent and is carried out by automated means.
- Right to withdraw consent (where processing is based on consent) without affecting the lawfulness of processing before withdrawal.
- Right to lodge a complaint with the Swedish Authority for Privacy Protection (IMY).

To exercise your rights, contact: it@logent.se. We may need to verify your identity. We normally respond without undue delay and at the latest within one month, unless an exception applies.

14. Security and incidents

Logent works systematically with information security. We use technical and organisational measures such as access controls, logging, backups, encryption where appropriate, training and incident management procedures. Personal data breaches are handled in accordance with internal procedures and reported to IMY when required.

15. Changes to this policy

We may update this policy as needed, for example when processes, systems or regulations change. In the event of material changes, we will inform affected parties.