Employee Privacy Notice

Last review: 22 October 2025
Status: Approved

Reviewer: Titus Halaczek
Owner: Titus Halaczek

Table of Contents

The purpose of this document....2
The kind of information we hold about you....3
How we collect your personal data....4
Security and Compliance....5
When we will use your personal data....7
How we use special categories of personal data....8
Data sharing....8
Transferring information outside the EU....9
Data security....10
Data retention....10
Your rights....10
Contact Us....11

The purpose of this document

In the context of your employment or engagement, Nexthink SA or its relevant affiliate ("**Nexthink**" or "**we**") is a 'data controller.' As a data controller, we are responsible for deciding how we collect and use personal data about you. We are required under data protection legislation to notify you of the information contained in this privacy notice.

As Nexthink includes a group of related companies, including Nexthink SA and its wholly-owned subsidiaries, the relevant entity operating as data controller will include at a minimum Nexthink SA, the Nexthink subsidiary directly employing you (if different), and any other such Nexthink entity that processes your personal data on behalf of Nexthink.

This notice applies to current and former board members, officers, representatives, employees, workers, contractors and certain service providers. This notice is informational and does not form part of any contract of employment or other contract to provide services. We may update this notice at any time in accordance with our publication process, at such times as we deem necessary to reflect changes or clarifications to practices and when otherwise required. Although we will endeavour to remind you, we encourage you to check back on this notice periodically so that you are aware of the most recent version.

The kind of information we hold about you

In the course of your employment or engagement, we may collect, store, and use personal data about you for your employment or engagement ("**Employee Data**"). The types of personal data we process include, but are not limited to:

- Identification data e.g., name, photograph, gender, date of birth, employee identification number;
- Contact details e.g., home address, telephone, email, emergency contact details;
- Employment details e.g., employment history, job title/position, grade, team, reporting lines, employment contract, dates of hire and termination, working hours, performance and disciplinary records, internal and external correspondence, calendar and appointment records, training and career development records, leave requests, parental leave, sickness records and holiday records;
- Professional qualifications achievements and skills information e.g., academic and professional qualifications, education, CV, references, languages;
- National identifiers e.g., national ID or passport, immigration status, driver's license;
- Spouse and dependents information – marital status and number of dependents, names, ages, contact details;
- Feedback from surveys e.g., skills, interests, personal data within the survey responses, and resulting analyses;
- Ethics and whistleblowing reports, which may include names, contact details, incident descriptions, timestamps, case identifiers, and other information you or a third party submits via the ClearView service, our externally hosted ethics and whistleblower reporting platform ("**Whistleblowing Platform**"). Reports may be submitted anonymously or with identifying details, depending on the reporter's choice;
- Financial information e.g., bank account details, tax information and social security information, salary and compensation, equity transactions, expenses;
- Benefits information e.g., employer pensions contributions, life assurance and private medical cover information, share options, bonuses;
- Pension information e.g., pension entitlements, early retirement information (if applicable);
- Nexthink device and IT related data ("**Use Data**") used to help us manage your devices, applications and our IT environment, assess performance and operational issues related to your device, applications and our IT environment, develop and improve our products and services, improve our software and provide IT support services to you

e.g., computer ID, user ID, IP addresses, service access logs, location, software and hardware inventory, cookies, login credentials, device and application analytics and history;

- Mobile device telemetry and usage diagnostics, collected from Nexthink's internal mobile applications (e.g., for testing or internal fleet insights), including battery metrics, memory usage, application performance, connectivity status, and device configuration data. Collection is limited to what is necessary for IT support and system health monitoring purposes.
- Employee performance data derived from quality assurance tools, including evaluations of support ticket interactions and similar service records. This may involve automated scoring, extracted metadata, tagging, managerial review inputs, and alert classifications.
- Travel and accommodation information within and outside of your local jurisdiction for business;
- Special Categories of Personal Data, e.g., records of accidents at work, fitness for work assessments, medical information acquired due to absence(s), disabilities, dietary requirements; Criminal records and background checks.

How we collect your personal data

Usually, you will have provided the information we hold about you but there may be situations where we collect personal data from other sources. Initially, Employee Data is collected through the introduction, recruitment and onboarding processes, either directly or sometimes from third parties, such as an employment agency or our background check provider. We may sometimes collect additional information from other unrelated third parties in the ordinary course or as required by your role, such as references from former employers, details from profile, skills or aptitude test providers and tax information from government authorities. Throughout your time with Nexthink, we will collect personal data, in the course of job-related activities and in support of our compliance obligations, from various sources, such as feedback from colleagues collected during performance appraisals, development of any performance improvement plans and/or in the creation of any disciplinary records, or corporate mobile phone data or feedback from survey providers.

Use Data is collected through your use of Nexthink-connected devices and your interaction with our IT systems.

We collect personal data about you from multiple sources throughout your employment lifecycle at Nexthink. Much of this data is provided directly by you, particularly during the recruitment, hiring, and onboarding processes. However, we may also obtain information from third parties, including recruitment agencies, background check providers, former

employers (e.g., references), and government authorities (e.g., tax and work eligibility information).

During your time with Nexthink, additional data is collected in the context of your job performance, engagement with tools and platforms, and participation in employee development and compliance programs. This includes data generated by:

- HR processes such as performance reviews, feedback from colleagues, learning and development activities, and disciplinary procedures.
- Corporate systems and applications, including email, collaboration tools, ticketing systems, and access management platforms.
- Devices and endpoints provided or managed by Nexthink (e.g., laptops, mobile devices) for operational diagnostics, security, or IT support purposes.
- External service providers used for employee engagement, surveys, or benefit administration.
- Internal tools such as quality assurance systems that evaluate service performance.
- Voluntary submissions, such as ethics or whistleblower reports submitted via the Whistleblowing Platform.

We also collect data from security systems that monitor Nexthink's IT environment for compliance with policies, detection of suspicious or anomalous behaviour, and identification of cybersecurity threats. These systems may include endpoint protection, identity and access management tools, and activity logging solutions.

In all cases, the scope of data collected is limited to what is necessary for legitimate business purposes and aligned with our internal policies and applicable law.

Mobile telemetry is collected directly from mobile devices through Nexthink applications installed via MDM or work profile deployment. No access is made to personal content or GPS data, and collection respects enterprise boundaries such as work profile limits.

Security and Compliance

Nexthink is subject to various security and compliance commitments for its delivery of IT products and services to customers and Nexthink employees and affiliates. Nexthink has committed as a company, as a service provider and employer, to meet the rigorous requirements of applicable law, industry certifications for best practices, GDPR-level implementation across jurisdictions and contractual obligations to our customers.

In connection with these standards, as they relate to our technology environments, we will continue to implement and manage a supervision program to reduce risk and gain oversight of our IT and communications systems and its individual hardware and software components.

We regularly deploy automated tools such as anti-malware software, website filtering and spam filtering.

As part of our security checks and protocols, Nexthink will also carry out oversight responsibilities with respect to its physical premises. Such oversight and risk management for physical premises may include using CCTV and badge scans, each potentially recording and logging related personal data and activity.

The primary purpose of these measures is to protect Nexthink, its employees, customers and business partners, for example:

- for general network operation and security, including in particular the security of Nexthink's IT systems and assets, and the optimal operation of its network and devices;
- for proof of business transactions and archiving;
- for coaching, training and evaluation of employees;
- for the protection of confidential information, trade secrets and other intellectual property;
- for investigating breaches of internal policies, fraud or other unlawful or wrongful activity, or to respond to a particular personnel or company incident;
- for business continuity (such as surveying business-related emails following an employee's departure); and
- for physical security of its premises.

Security and compliance activities are likely to be continuous and ongoing. However, they will be proportionate, for legitimate purposes and as required or permitted by applicable law. Before undertaking any security and compliance activities, we will consider your reasonable expectations of privacy and assess whether there are any alternative approaches.

You should be aware that any message, files, data, document, facsimile, telephone conversations, social media post or instant message communications, or any other types of information transmitted to or from, received or printed from, or created, stored or recorded on our IT and communications systems and assets are presumed to be business-related and may be inspected by us in accordance with applicable law.

You must clearly identify private emails and messages by adding the term "private and confidential" in the email or message's subject line, and/or storing those emails/messages/files in a separate folder marked "private and confidential". Without such clear identification, the content of such communications or files will be deemed business related and property of Nexthink. However, in cases of clear identification, Nexthink will take appropriate action to protect strictly personal data and minimize any disclosure; provided, however, Nexthink will exercise its professional discretion, under internal or external legal

counsel, and reserve its rights in certain cases: such as where such content may implicate a particular risk or threat to the company, or person; contain Nexthink confidential information or property; violate Nexthink permitted practices or policies; subject of a lawfully-issued subpoena; or access to such content is based on a separate legal authority.

When we will use your personal data

We will only use your personal data when allowed by law and for legitimate business purposes. For your information, standard processing grounds for processing personal data include the following:

- To manage the employment relationship (e.g., hiring, payroll, benefits, promotions, performance, and training).
- To meet legal or regulatory obligations (e.g., tax, immigration, health and safety, or reporting requirements).
- To operate corporate systems and infrastructure, including IT service delivery, communication platforms, and collaboration tools.
- To monitor the use of company systems and ensure compliance with Nexthink's internal policies and procedures.
- To detect and respond to security incidents, prevent fraud, and protect the integrity of Nexthink's IT environment.
- To support employee development and coaching through performance reviews, feedback mechanisms, and quality assurance tools.
- To analyse organisational effectiveness and employee engagement, including through internal surveys or feedback platforms.
- To investigate concerns raised via internal reporting channels or through the Whistleblowing Platform.

Where processing relies on our legitimate interests, we always balance these against your rights and freedoms and apply appropriate safeguards. We do not use personal data for solely automated decision-making that produces legal or significant effects without human involvement.

Where you choose to report an issue via the Whistleblowing Platform, we process such personal data in line with our legal obligations under whistleblower protection laws and our legitimate interest in maintaining a compliant, transparent workplace culture. Anonymous reports are supported and processed without identifying the reporter unless voluntarily disclosed.

How we use special categories of personal data

In general, we will not process information that reveals your racial or ethnic origin, religious, political or philosophical beliefs, trade union membership, information about your health/sex life, genetic data or biometric data for the purposes of unique identification ("**Special Categories of Personal Data**") unless it is necessary for performing or exercising obligations or rights in connection with employment, including:

- information about your health and disabilities, for example, to ensure your health and safety in the workplace and to assess your fitness to work, including routine drug testing, where appropriate and relevant to the position, pursuant to our Drug Testing Policy, to monitor and manage sickness absence and to administer benefits. We need to process this information to exercise rights and perform obligations in connection with your employment.
- information about your race or national or ethnic origin, religious, philosophical or moral beliefs, or your sexual life or sexual orientation, to ensure meaningful equal opportunity monitoring and reporting.

For certain roles, sensitive information about criminal convictions and background qualifications or activities will be used to comply with the requirements of some customers and partners (including highly confidential, regulated or classified entities, or public sector, and government organizations, as examples) to have our employees' backgrounds checked.

Data sharing

We will share your personal data with third parties where required by law, where it is required to confirm our compliance with applicable laws, where it is necessary to administer the working relationship with you or where we have your consent or a legitimate interest in doing so. We do so on a "need to know basis" and in accordance with applicable data protection law.

"**Third parties**" includes third-party service providers, independent auditors as well as other entities within our group. Activities that are carried out by third-party service providers include payroll, benefits, pension and expenses administration, IT support, employee performance management systems, and tools such as Salesforce, Jira or Microsoft. We will share your personal data with other members of the Nexthink group to administer human resources, employee compensation and benefits, as well as for other legitimate business purposes (such as IT services/security, tax and accounting purposes, general business and personnel management). All our third-party service providers and other entities in the group are required to take appropriate security measures to protect your personal data in line with our policies.

Finally, we may disclose certain portions of personal data to a competent law enforcement authority, government agency or court where We are convinced disclosure is necessary (i) as an obligation under applicable law or regulation, (ii) to protect your vital interests or those of any other person, or (iii) to exercise, establish or defend our legal rights.

Transferring information outside the EU

Nexthink is a global group of companies headquartered in the USA and Switzerland. Therefore, we may need to transfer personal data between these countries, in particular, to our head office for management purposes, as well to other countries where we operate, including the USA, UK and India. We also use third party service providers located in different countries. We have implemented safeguards for such transfers to comply with applicable laws such as the Standard Contractual Clauses approved by the competent authorities and public bodies to enable the transfer.

Nexthink, Inc. is committed to upholding data privacy standards in accordance with the EU-U.S. Data Privacy Framework ("**EU-U.S. DPF**"), the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. Data Privacy Framework ("**Swiss-U.S. DPF**") as established by the U.S. Department of Commerce. Nexthink, Inc. has formally certified to the U.S. Department of Commerce its adherence to the EU-U.S. Data Privacy Framework Principles ("**EU-U.S. DPF Principles**") concerning the processing of personal data received from the European Union under the EU-U.S. DPF and from the United Kingdom (including Gibraltar) under the UK Extension to the EU-U.S. DPF. Additionally, Nexthink, Inc. has certified its commitment to the Swiss-U.S. Data Privacy Framework Principles ("**Swiss-U.S. DPF Principles**") in relation to the processing of personal data received from Switzerland under the Swiss-U.S. DPF. In the event of any discrepancies or conflicts between the terms outlined in this privacy policy and the EU-U.S. DPF Principles and/or the Swiss-U.S. DPF Principles, the principles established in the EU-U.S. DPF and Swiss-U.S. DPF shall take precedence and govern our data privacy practices. To learn more about the Data Privacy Framework (DPF) program, and to view our certification, please visit https://www.dataprivacyframework.gov/. The Federal Trade Commission has jurisdiction over Nexthink, Inc. compliance with the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. DPF.

If your personal data is subject to the GDPR, UK GDPR or the Swiss FADP and We intend to transfer the respective information to a third-party service provider and/or partner based in a jurisdiction subject to the privacy laws and regulations of a foreign jurisdiction, We will (i) enter into a contract with such party, (ii) transfer the information only for limited and specified purposes, (iii) ascertain that an adequate transfer mechanism is in place, such as the DPF or the Standard Contractual Clauses, (iv) take reasonable and appropriate steps to ensure that the party effectively processes the information in a manner consistent with Our obligations under the applicable transfer mechanism, (v) require the it to notify Us if the party determines that it can no longer meet its obligation to provide the level of protection required by the

applicable transfer mechanism, (vi) upon notice take reasonable and appropriate steps to stop and remediate unauthorized processing of the information, and (vii), where the DPF is the applicable transfer mechanism, provide a summary or representative copy of the relevant privacy provisions of the service provider's or partner's contract to the Department of Commerce, upon its request. We remain liable if Our third-party Processor onward transfer recipients process relevant personal information in a manner inconsistent with the applicable transfer mechanism, unless We prove that We are not responsible for the event giving rise to the damage.

Data security

We have put in place appropriate security measures to prevent your personal data from being accidentally lost, used or accessed in an unauthorized way, altered or disclosed. We have put in place procedures to deal with any suspected data security breach and will notify you and any applicable regulator of a suspected breach where we are legally required to do so.

Data retention

We will only retain your personal data for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements, or as otherwise required by contractual agreements with third parties, law or other Nexthink policies. Details of retention periods for different aspects of your personal data are available in our Data Retention policy which is available on the Employee Portal.

Your rights

It is important that the personal data we hold about you is accurate and current. Please keep us informed if your personal data changes during your working relationship with us.

Under certain circumstances, by law you may have the right to:

- request access to your personal data;
- request correction of the personal data that we hold about you;
- request erasure of your personal data;
- object to processing of your personal data;
- request the restriction of processing of your personal data; and
- request the transfer of your personal data to another party.

If Nexthink is relying solely on your consent to process your personal data, you have the right to withdraw your consent at any time. This will not, however, affect the lawfulness of the processing before your consent has been withdrawn.

If you want to review, verify, correct or request erasure of your personal data, object to the processing of your personal data, or request that we transfer a copy of your personal data to another party, please contact the Privacy Team at dl-privacy@nexthink.com.

You have the right to complain to a data protection authority about our collection and use of your personal data, although we ask that you raise your objects internally in the first instance. Please contact us in the first instance using the details below and we will attempt to resolve your complaint. However, if you remain dissatisfied after our response, you may contact your local data protection authority. With regard to any unresolved complaints concerning our handling of personal data received by Nexthink, Inc. in reliance on the EU-U.S. DPF, the UK Extension to the EU-U.S. DPF and the Swiss-U.S. DPF, we commit to cooperate and comply respectively with the advice of the panel established by the EU data protection authorities, the UK Information Commissioner's Office (ICO) and the Gibraltar Regulatory Authority (GRA), and the Swiss Federal Data Protection and Information Commissioner (FDPIC). You may have the option to select binding arbitration under the EU-U.S. Data Privacy Framework Panel for the resolution of your complaint under certain circumstances.

Contact Us

If you have any questions about this Privacy Notice, our treatment of your personal data, or need to access this Privacy Notice in an alternative format due to having a disability, please reach out to our Privacy Team and Data Protection Officer at dl-privacy@nexthink.com.

***