# The Kyndryl privacy baseline

Our privacy baseline describes the principles and practices we rely on to protect the personal data of our employees, customers, and other third parties. These guidelines are designed to meet or exceed the requirements of current privacy laws in all countries where Kyndryl does business and are updated as necessary to account for new and evolving regulations.

> "Kyndryl is committed to the highest standards of data governance. Our privacy baseline enables our global organization to operate seamlessly across borders with uniform practices, providing you with the reassurance that we will always handle your data in a secure, lawful, and transparent manner."
>
> Nuzhat Sayani,
> Kyndryl Chief Privacy & Data Governance Officer

## Part I: Kyndryl data

This part outlines how we manage data that we control, including the personal data of our employees and the business contact information of our customers, partners, and other third parties that interact with us.

### Kyndryl privacy fundamentals

**Kyndryl's data privacy policy and processing principles**

Our Privacy Principles govern how we collect, use, disclose, store, access, transfer or otherwise process personal data:

- **Fairness**: We collect and process your personal data in a fair, lawful, and transparent manner.
- **Purpose Limitation**: We collect your personal data for specific, explicit and legitimate purposes and process it only in ways compatible with those purposes.
- **Data Minimization**: We limit personal data processing to what is adequate, relevant and necessary for the intended purposes.
- **Accuracy**: We keep your personal data as accurate, complete and up to date as necessary for the intended purposes.
- **Retention**: We retain your personal data only for as long as necessary to fulfil the intended purposes.
- **Disclosure**: We share your personal data internally or externally only when appropriate and in compliance with applicable data protection laws.
- **Security**: We implement appropriate technical and organizational measures to protect your personal data from unauthorized or unlawful access and from accidental loss, destruction or damage. Third parties are instructed to process your personal data in a manner consistent with the Kyndryl privacy baseline.
- **Individual Rights**: We respect your privacy rights, including the rights of access and correction, in accordance with relevant data protection laws.

- **Custodianship**: We ensure safe handling of your personal data.
- **Accountability**: We demonstrate compliance with applicable data protection laws through proper governance, policies, training and oversight.

**Kyndryl privacy statements**

- **External privacy statement**
  When we collect your personal data, we provide notice of our privacy policy through our External Privacy Statement which informs you of your rights and describes how we collect, use, share, and protect your personal data. This statement applies to Kyndryl and its subsidiaries, unless a subsidiary presents its own statement without reference to Kyndryl's.
- **Internal privacy statement**
  Our Internal Privacy Statement provides notice of how we may use our employees' personal data. It describes the general privacy practices that apply when we collect, use, and share the personal data of our employees, contractors and other individuals who we work with.

## Conditions for the processing of Kyndryl personal data

The Kyndryl privacy baseline provides operational guidelines for Kyndryls who are responsible for compliance with our Data Privacy Policy & Processing Principles and applicable privacy laws when processing Kyndryl personal data.

**Privacy by design and by default**

We integrate privacy principles into every stage of the data processing lifecycle. This approach applies to all activities involving the processing of personal data, whether automated or manual.

**Data subject rights management**

We have mechanisms and procedures in place to ensure that individuals can exercise their rights under applicable data protection laws. This includes providing clear, accessible channels for submitting requests to access, rectify, erase, restrict, or object to the processing of personal data, and ensuring these requests are addressed promptly and efficiently.

**Data sharing, transfers and disclosure**

We strictly control data sharing, transfers, and disclosure within Kyndryl through policies designed to ensure the confidentiality, integrity, and availability of information. We use approved tools for communication and data transfer, and specific policies and safeguards govern data transfers outside Kyndryl. For cross border transfers, we use mechanisms such as EU Standard Contractual Clauses and the APEC Cross Border Privacy Rules (CBPR) system.

Additionally, Kyndryl is certified under the EU-U.S. Data Privacy Framework, the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. Data Privacy Framework.

**Data retention and disposal**

Our approach to data retention and disposal specifies how long various categories of personal data will be kept and outlines the procedures for securely disposing of data that is no longer needed. This minimizes the risks associated with obsolete or redundant data, ensuring personal data is retained only for as long as necessary to fulfil the purposes for which it was collected and disposed of securely to prevent unauthorized access and misuse.

## Privacy risk assessment

Our privacy framework requires owners of all internal applications, processes, and tools that handle personal data to complete a Global Privacy Assessment and maintain accurate Records of Data Processing Activities. These

assessments provide transparency into how personal data is processed and help identify and mitigate potential privacy risks and vulnerabilities relating to the processing activity.

We further scrutinize applications and processes identified as medium or high risk through our dedicated Data Governance Assessments team. These applications and processes are subject to ongoing audits, including, where appropriate, an in-depth Data Protection Impact Assessment (DPIA).

## Security measures

**Cybersecurity**

The Kyndryl Cybersecurity Policy ensures a standardized approach to implementing security policies and controls across the company.

Aligned with the internationally recognized ISO/IEC 27002:2022 standard and incorporating many provisions of the European NIS2 directive, this policy details the organizational, people, physical, and technological controls that must be implemented across all Kyndryl IT systems and environments, without exception.

**Encryption**

Encryption is a cornerstone of our data protection strategy. We have implemented policies and controls to encrypt personal data based on its sensitivity and associated risks, including privacy concerns related to cross-border transfers. We mandate encryption when transferring sensitive personal data (SPI). Where effective end-to-end encryption is necessary to protect personal data stored in or accessed from a location deemed inadequate for such data, the data remains strongly encrypted at all times, both in transit and at rest. We securely store encryption keys in an appropriate location to prevent unauthorized access.

**Data breach management**

We have established procedures that outline the measures and controls required to safeguard personal data from unauthorized access, disclosure, alteration, or destruction. These include specific measures for detecting, reporting, and responding to data breaches. In the event of a data breach, we are committed to taking immediate and effective action to mitigate harm and fulfil all notification requirements to the relevant Authorities and to the individuals impacted.

## Employee privacy education and training

Kyndryl employees who access personal data adhere to the principles outlined in the Kyndryl Code of Conduct and the Kyndryl privacy baseline.

We provide education on best practices for data protection and the risks associated with mishandling data. Annual cybersecurity, data privacy and AI ethics education is mandatory for all employees, with training materials available for ongoing reference.

Kyndryl managers ensure their direct reports and contractors complete the mandatory corporate privacy compliance and information security training in a timely manner. Managers also ensure that employees who access or handle personal data complete role-based training tailored to their responsibilities.

Kyndryl employees are informed that non-compliance by Kyndryl employees and our extended workforce personnel may result in disciplinary action.

## Monitoring and auditing

Monitoring and auditing are essential for maintaining ongoing compliance with regulations, identifying and mitigating privacy and security risks, and maintaining the integrity of personal data. We conduct periodic privacy audits to ensure adherence to the Kyndryl Privacy Policy and Guidelines.

We also maintain logs of data access and modifications to detect any unauthorized activities. Strict access controls are in place to monitor who can access sensitive data, and automated alerts are implemented to flag unusual or suspicious activities.

# Part II: Customer data

This part outlines how we manage and process personal data that our customers and other third parties entrust us to process on their behalf.

## Conditions for the processing of customer personal data

The Kyndryl privacy baseline provides operational guidelines for Kyndryls who are responsible for compliance with our internal policies and applicable privacy laws when processing customer personal data.

Regardless of any customer obligations in our contracts, these guidelines serve as the baseline for all our customer services, providing all our customers with more control over how Kyndryl manages and protects their data.

**Customer agreement**

Where we process customer personal data, we enter into a Kyndryl Data Processing Addendum (DPA). Any modifications or exceptions to the Kyndryl DPA must be approved by Kyndryl Legal.

**Processing description**

We prepare one or more Data Processing Addendum (DPA) exhibit(s) that detail the processing of customer personal data for each customer transaction or group of customer transactions.

**Use and reuse of customer personal data**

We only process customer personal data for the purposes explicitly specified in the contract between us and the customer, and as instructed by the customer. We do not use or reuse customer personal data for other Kyndryl purposes without customer agreement.

**Notification of infringing instructions**

We review every new instruction from our customers for processing and inform the customers if we believe that the processing instructions infringe applicable privacy laws.

**Return or disposal of customer personal data**

We retain customer personal data only as long as necessary to fulfil the contractual obligations in accordance with the customer's instructions. Upon termination or expiry of the contract, we return or delete the customer personal data, as agreed with the customer. Any exceptions must be approved by Kyndryl Legal.

**Customer assistance**

Taking into account the industry, the regulatory environment of the customer, and the agreed scope of the services, we document and implement processes to comply with Kyndryl's assistance obligations, as defined in the customer contract and the Kyndryl Data Processing Addendum.

## Privacy by design and by default

Privacy by design and by default requires that privacy requirements are identified prior to processing and controls implemented at all stages of the processing lifecycle, to ensure that the processing of personal data meets legal and regulatory requirements. These controls fall into two categories:

- **Universal controls**: Controls implemented for all processing of customer personal data.
- **Processing dependent controls**: Controls where the responsibility for compliance lies with the data controller who is usually the customer. However, depending on the nature of the services, the customer may be partially or completely dependent on us to fulfil the requirements.

## Universal controls

We apply universal privacy by design and by default controls to all Kyndryl activities that involve the processing (including use, disclosure, retention, transmission and disposal) of customer personal data, either by automated or manual means, including operational services such as support and maintenance.

### Roles and responsibilities

We define (and document) roles and responsibilities to ensure we meet our obligations for the contracted services we provide.

### Data minimization

We process only the minimum amount of customer personal data necessary to deliver the contracted services across the entire processing lifecycle.

### Access limitation to data

We design and implement access controls so that only those individuals who require access to personal data to deliver the contracted services are authorized to do so.

### Risk assessment and review

The Kyndryl Data Processing Addendum (DPA) refers to the DPA exhibit regarding the details of the Technical and Organizational Measures (TOMs). While the specific TOMs need to be agreed with the customer, our Data Security and Privacy Principles (DSP) serve as a baseline.

The roles and responsibilities with respect to TOMs are outlined in the customer contract.

### Secure deletion

We implement customers' instructions to delete customer personal data residing on IT resources or media that is decommissioned or disposed of in accordance with the NIST guidelines for media sanitization (SP 800-88 rev. 1), as contracted.

### Secure data transfers

We implement the specific TOMs agreed with customer to transfer customer personal data internally or externally such that it reaches its intended destination in a secure manner.

### Personal data handling procedures

We document procedures for the secure and compliant handling of customer personal data and make the documentation available to our staff processing personal data. These procedures will be appropriate to the

individual's role, responsibilities, and tasks and consistent with the requirements of the Kyndryl Cybersecurity Policy, the controls in this document and any contractual obligations for the handling of customer personal data.

**Privacy configuration guidance**

We provide documentation that enables authorized individuals to understand the technical settings, configuration, administration, and user options that enable the tools used for the provision of the contract services to be set up, administered, and used in a secure and privacy-optimized way.

**Logging and monitoring**

We implement logging and monitoring to support threat detection and investigation, and log access to customer personal data (as collected by us as part of the contracted services provided to the customer), including by whom, when, and what (if any) changes were made (additions, modifications, or deletions).

**Encryption**

Where the infrastructure we support as part of the contracted services is intended to store customer personal data, we encrypt data in transit by default and at rest when this is part of the contracted services, provide the customer with the option to encrypt, or recommend that the customer enable data encryption at rest, where appropriate.

**No personal data in test data**

We do not use data containing customer personal data for testing purposes. Synthetic data is used, unless all the following criteria are met:

- Customer permission is obtained in writing.
- TOMs in the testing environment are equivalent to those in production (including deletion from the test system when testing is completed).

**Role-based education and training**

Our employees and contractors who have access to, or handle customer personal data complete role-based training appropriate to their roles, responsibilities, and tasks (including on cybersecurity, privacy, and AI). Separate trainings are usually provided to accompany the introduction of process changes or new processes due to technological developments, changes in laws, regulations and best market practice.

**Change management**

We manage and control changes to contracted services that materially impact the processing of customer personal data, ensuring that DPA exhibits are updated every time a change in the processing activities takes place and prior to the new processing activities taking place.

**Data backup and recovery**

We implement contracted backup and restore controls, except where the responsibility is contractually assumed by the customer.

## Processing dependent controls

Generally, the responsibility for customer personal data controls lies with the customer.

**Personal data collection and generation limitation**

We follow customer instructions as agreed in the contract to ensure that only the minimum necessary customer personal data is collected or generated for the duration of the contracted services.

**Personal data accuracy and quality**

We assist the customer to maintain the accuracy and keep the customer personal data up to date, when such assistance is part of the contracted services.

**Data return or destruction**

We document as part of the customer contract how data is returned to the customer or destroyed upon termination of the contracted services. When appropriate, we enable the customer to control and manage the retention and disposal of the customer personal data processed during the provision of the contracted services.

**Ability to locate data**

We document our hosting locations, including back-up locations, to enable our customers to easily locate their personal data.

## Supporting customer data subject rights

The Kyndryl Data Processing Addendum sets out our commitment to assist our customers in fulfilling data subject rights requests and other legal obligations and, where appropriate, how we will be compensated for such assistance.

## Data sharing, transfers and disclosures

**Records of processing locations, entities, and transfers**

We prepare DPA exhibits for each customer transaction or group of customer transactions that include an accurate and complete list of all subprocessors (Kyndryl and third-party) and their processing locations.

We verify that the processing locations listed in a DPA exhibit for subprocessors are countries that Kyndryl considers having adequate data protections for the nature of the proposed processing. Further, we implement Supplementary Measures for industry sectors in certain countries where required.

**Basis for transfer across jurisdictions**

As a global company, we have implemented measures to govern the international transfer of personal data and ensure an adequate level of data protection.

Intercompany transfers are governed by Kyndryl's internal intercompany agreement including the Standard Contractual Clauses (SCC) and Transfer Impact Assessment (TIA) where required by applicable data protection law and outlined in the Kyndryl DPA. Both are also part of Kyndryl's third-party subprocessor engagement process. In addition, **Kyndryl is certified under the EU-U.S. Data Protection Framework**.

**Disclosure of the use of subprocessors**

We will update the DPA exhibit, or equivalent contractual document agreed with the customer, to list the subprocessors used for the processing of customer personal data prior to their involvement.

We will inform customers before involving new or replacing existing subprocessors as per the process agreed in the DPA exhibit.

**Engagement and contracts with subprocessors**

All our vendors and subprocessors undergo a privacy and security assessment as part of the engagement process and we instruct them to process personal data consistent with the Kyndryl privacy baseline.

Where customers' or subprocessor terms deviate from Kyndryl standards, we ensure that any deviating obligations between the respective parties are, to the extent applicable, agreed back-to-back by flowing down the deviating customer requirements to the subprocessor or – in exceptional cases – flowing up the deviating subprocessor terms.

**Oversight of subprocessors**

We and our third-party subprocessors are subject to audits carried out by our procurement and internal audit teams who work closely with our Chief Privacy & Data Governance Officer, especially when defining the control objectives.

We conduct periodic monitoring and review of third-party subprocessors' privacy and security capabilities, and perform additional monitoring and reviews, if appropriate.

**Disclosure request management**

Our Legal team will promptly handle all requests from regulatory authorities (for example, data protection authorities, regulators, and law enforcement agencies) for the disclosure of customer personal data or for information related to the processing of customer personal data in accordance with our policy for Government Requests for Customer Data.

**Incident management**

We have established procedures for the identification and reporting of security and privacy incidents involving customer personal data.

Incidents are reported centrally to the Kyndryl Cyber Security Incident Response Team (CSIRT), an international team of experts who lead investigations and support our internal teams in taking immediate mitigation actions and strengthening prevention strategies. CSIRT works closely with our Chief Privacy & Data Governance Officer who acts in an advisory capacity and as a point of contact for cooperation with the competent data protection authority.

Where incidents concern customer personal data, we inform customers in accordance with the agreed contract terms. Please see the Kyndryl Data Processing Addendum (DPA) for details of our standard terms. The incident notification process is part of our mandatory Cybersecurity, Privacy and AI education and training.

If you have any questions related to privacy at Kyndryl, please contact us by using this form.