Microsoft's Employee Privacy Principles

Microsoft believes that privacy is a fundamental human right. It is core to our business that consumers and enterprises alike trust us with their data. With trust, we can empower every individual and organization on the plant to achieve more.

Similarly, respecting these principles in the workplace empowers our employees to do their best work. Our employees power our mission each and every day. Their trust is essential if we are to achieve that mission. We firmly believe that employees do not fundamentally give-up their privacy rights by virtue of their employment at Microsoft. We respect the privacy laws and requirements of every country where we operate. In many cases, Microsoft goes beyond what is required to ensure that our employees can truly trust that Microsoft will act responsibly with the data we gather about them and remain our Company's greatest champions and advocates.

In short, ***Microsoft takes a thoughtful, considered and deliberate approach to employee privacy*** that both acknowledges the uniqueness of the employment relationship while also balancing the Company's interests in running a secure, inclusive, efficient, and innovative operation. Our approach is bolstered by a privacy program that cares deeply about these issues, as reflected in Microsoft's investment in its Employee Data Governance Board (EDGB), who oversees the requirements of the Microsoft Privacy Standards concerning employee data, and partners across Microsoft's established privacy program to ensure teams treat employee privacy with extraordinary care.

The employment relationship is different from a consumer or customer relationship, and will at times mean that Microsoft has contractual, legal or other requirements to use employee data, including to provide required government reporting (such as reports required of Microsoft as a federal contractor, or pay-gap reporting in some countries), or take appropriate action to defend or prosecute legal claims made against or by the Company.

Informed by both our desire to maintain trust and balance the different nature of the employment relationship, Microsoft has adopted six core employee privacy principles:

I. **Microsoft provides notice about how employee data is used.**

Microsoft first and foremost believes employees should have clear and appropriate notice about how employee data may be used. That notice starts with Microsoft's Data Privacy Notice for Employees, External Staff, Candidates and Guests (DPN). The DPN and its addenda set out the framework for all of Microsoft's processing of employee data. If you have not yet taken the opportunity to review the DPN, we encourage you to do so. The DPN and its addenda are updated annually, and employees are reminded of the DPN on an annual basis through required privacy training.

In addition to the DPN, Microsoft will provide more specific privacy notice when it is required. For example, our Elite dogfooding program frequently provides additional notice about the kinds of data being gathered when dogfooding new products. Additionally, your local employment contract or employee agreement may also contain provisions related to data processing.

II. When possible, Microsoft offers choice on how employee data is used.

While Microsoft does not rely on consent for processing most employee data (unless legally required), we do believe in offering employees choice as to how that data is processed, where appropriate. That choice can take many forms. In some cases, it's offering employees the ability to opt-out of certain kinds of product features, or certain truly optional data uses. The Microsoft Data Program (MDP) is a good example of this kind of choice. You can read more about that program in the MDP Addendum to the DPN. That program generally leverages approved Microsoft business data for product development and improvement, subject to a number of controls and limitations. Employees in countries where the program is active are offered the ability to choose not to participate in the program entirely, or to take steps to limit the kinds of data processed by that program.

The unique nature of the employment relationship means that choice may be more limited or not available for certain kinds of data processing (payroll processing for example). Similarly, where Microsoft has legal or contractual rights or obligations to process or disclose data, we cannot allow for choice in how that data is used.

III. Microsoft thoughtfully balances employee and company interests when using data.

Where processing of employee data is not wholly supported by legal, contractual or other specific requirements, Microsoft carefully considers its interests in using the data, and balances that interest against an individual employee's privacy interests in the data. In particular, when it comes to using business data for certain kinds of optional or "secondary" uses, like product development or business insights, Microsoft deeply considers the impact such use may have on employee privacy, and what controls it can and should establish to protect employee privacy before proceeding. Microsoft might, for instance, provide opportunities to opt-out of particular data uses, ensure data is de-identified, pseudonymized or anonymized before use, or implement other kinds of security measures and controls to ensure appropriate use of the data.

A good example of this is in our design and implementation of Viva Insights, which leverages data to surface insights directly to you to help you make decisions about how you are investing your time at work. These insights are not shared with your manager at an individual level, quite deliberately, to keep the insights at an appropriate team or group level as part of our commitment to employee privacy.

IV. Use of employee data is appropriately limited and controlled.

When Microsoft does make use of data it takes reasonable steps to ensure that we only use the data needed to fulfill a particular use. For example, we ask teams who want to use data for product development or experimentation to tailor their data needs to those that are strictly necessary for their work. Teams seeking to use our data must comply with existing privacy requirements or engage in rigorous processes that review access to, and uses of, employee data to ensure appropriate minimization and scope of use. Access to data that is not necessary to support the intended scope is generally prohibited.

V. Microsoft provides access to employee data.

Microsoft routinely provides its employees access to their own data, like their pay, benefits, vacation time, Rewards and Connects through self-service portals. Microsoft also provides employees additional access to their individual data at the employee's request, to the extent required by local law. Giving

employees self-service access to, and the ability to make corrections and updates to that data as appropriate, ensures employees always have access to the data they care about most.

VI. Employee data is protected by industry leading security safeguards.

In addition to privacy, the security of our employee data is paramount. Data related to our employees is carefully controlled. We minimize access to more sensitive data, like that used by our HR teams, to those who truly have a business need to work with it and require teams to respect existing privacy requirements, or engage in a privacy review, for new uses of data to ensure they are appropriate. Our employee data is also considered “customer data” by our engineering teams, requiring appropriate review, approval and controls before Microsoft would allow that data to be used.

Last updated: January 31, 2023