

GDPR — Legitimate Interest Assessment

Internal Use of Microsoft Teams

Contents

1 Legitimate Interest Assessment for the Use of Microsoft Teams	3
1.1 Purpose Test	3
1.2 Third-Party Benefits from the Processing	3
1.3 Potential Impact of Non-Processing	4
2 Necessity Test	4
2.1 Streamlined Communication and Collaboration	4
2.2 Remote Meeting Coordination	4
2.3 Real-Time Document Collaboration	4
2.4 Integration with Existing IT Infrastructure	5
3 Balancing Test	5
3.1 Nature of Data Processed	5
3.2 Expectation of Processing	5
3.3 Intrusiveness and Potential Impact	6
3.4 Pre-existing Relationship	6
3.5 Safeguards and Consent	6
4 Potential Risks to Data Subjects Related to the Use of Microsoft Teams	7
4.1 Unauthorised Access and Data Breaches	7
4.2 Data Retention and Deletion	7
4.3 Data Transfer Outside the EU	7
4.4 Third-party App Integrations	7
4.5 Profile Building and Analytics	7
4.6 Eavesdropping and Surveillance	7
4.7 Lack of Awareness Among Users	7
5 Mitigation	7
5.1 Data Encryption	7
5.2 Access Controls	8

5.3	Regular Review of Permissions	8
5.4	Employee Awareness and Training	8
5.5	Compliance with Microsoft's Best Practices	8
5.6	Data Retention Policies	8
5.7	Incident Response Plan	8
6	Review	9
6.1	Frequency	9
6.2	Triggers for Review	9
6.3	Review Process:	9
7	Transparency	10
7.1	Purpose and Implementation	10
7.2	Communication Channels	10
7.3	Content of Communication:	10
7.4	Privacy Notice Update	11
8	Conclusion	11

1 Legitimate Interest Assessment for the Use of Microsoft Teams

1.1 Purpose Test

The primary purpose of processing personal data by means of Microsoft Teams is to facilitate and improve organisation-wide communication and collaboration. This purpose can be broken down into the following specific objectives:

1.1.1 Efficient Internal Communication

With the rise of remote working and teams being spread across different locations, there's a growing need for real-time, digital communication tools that are more dynamic than email.

JUSTIFICATION: With Microsoft Teams, employees can instantly send messages, and they can do that using multiple devices, reducing delays that can occur with other means of communication. This immediacy is essential for prompt decision-making, immediate feedback, or urgent company-wide announcements.

1.1.2 Collaboration Among Employees

Beyond simple communication, the tool enables multiple users to work on a single document simultaneously in dedicated channels, join group chats themed around specific topics or projects, and create channels for department-specific needs.

JUSTIFICATION: Such collaborative tools minimise the back-and-forth that might be seen with traditional methods, like emailing documents for review. It promotes teamwork, ensures all team members are on the same page, and reduces the time to finalise work and team projects.

1.1.3 Coordination and Hosting of Remote Meetings

Microsoft Teams is not just a chat tool; it also

provides video conferencing features. This is essential for hosting team meetings, one-on-one check-ins, or even larger webinars or training sessions.

JUSTIFICATION: In a globalised world and a post-pandemic environment, the ability to host and join meetings remotely is crucial. It saves time, reduces travel costs, and ensures continuity of operations even if physical presence is not possible.

1.1.4 Real-time Information and Document Sharing

Microsoft Teams integrates with the Microsoft Office suite of products, allowing users to share, edit, and discuss documents without leaving the platform.

JUSTIFICATION: This seamless integration reduces the complexity and time required to switch between multiple tools. It ensures that all team members have access to the latest version of a document, thereby reducing errors and inconsistencies.

In essence, the legitimate interests in using Microsoft Teams revolve around the need for efficient communication, seamless collaboration, and the practicalities of modern work environments. Given the digital nature of most businesses today, such tools are nearly indispensable in ensuring smooth operations.

1.2 Third-Party Benefits from the Processing

Whilst the use of Microsoft Teams is essential for communication and collaboration within a particular organisation, communication itself is only a means to achieve certain, commercial,

or non-commercial, objectives. On that basis, in most cases, third parties outside the organisation (such as customers, business partners, recipients of public services etc.) indirectly benefit from the processing of personal data by means of Microsoft Teams.

1.3 Potential Impact of Non-Processing

Microsoft Teams is one of the most popular communication and collaboration platforms used by organisations across both the public and private sectors. If they decided not to use Micro-

soft Teams anymore, it would likely hinder their business operations significantly. Employees would be unable to communicate and cooperate smoothly, which could result in considerable delays in delivering work output because of a lack of sufficient information sharing. Employee engagement at work would be significantly impacted. The impact would be even heavier for organisations with a presence in multiple countries, for which Microsoft Teams (or equivalent tools) are currently the primary means of internal communication.

2 Necessity Test

The use of Microsoft Teams is considered necessary for the efficient management and operations of our organisation for the following reasons:

2.1 Streamlined Communication and Collaboration

For a modern organisation, especially those offering remote or hybrid work models, having an integrated tool for communication is indispensable. Email, while valuable, isn't suitable for real-time communication or instant collaboration on projects.

2.1.1 Assessment

Is Microsoft Teams essential? While it's possible to communicate via email or even phone calls, these methods don't offer the immediacy and integrative features Teams does. The real-time chat, combined with file sharing and multi-participant video meetings in one platform, is vital for efficiency. Thus, using a platform like Teams is necessary for effective and streamlined communication.

2.2 Remote Meeting Coordination

Hosting and coordinating remote meetings have become a cornerstone of modern business operations. While there are multiple tools available for this, integrating it with a communication tool simplifies the process.

2.2.1 Assessment

Could our organisation use separate tools for chatting and video conferencing? Yes, but it introduces complications. A singular platform like Teams, where employees can shift from a chat to a video call, simplifies workflows and is necessary for smooth operations in a fast-paced business environment.

2.3 Real-Time Document Collaboration

Microsoft Teams allows multiple users to collaborate on a document simultaneously, ensuring everyone has the latest version and can provide immediate feedback.

2.3.1 Assessment

Are there alternatives to this feature? While standalone document collaboration tools exist, e.g. Sharepoint or OneDrive, integrating them within a communication platform enhances efficiency. The necessity here is to avoid fragmented workflows and ensure consistent access to up-to-date files. In addition, the ability to share documents within predefined groups of people in Teams takes away the hassle of having to maintain access rights to documents on dedicated file-sharing platforms.

2.4 Integration with Existing IT Infrastructure

Microsoft Teams integrates seamlessly with other Microsoft products and many third-party tools. For companies already invested in the Microsoft ecosystem, using Teams is a logical choice.

2.4.1 Assessment

Is this integration necessary? For companies deeply rooted in the Microsoft ecosystem, switching to another tool or not making use of the best available options, i.e. Teams, might result in disruptions, decreased productivity, and increased training requirements. Thus, using Teams becomes necessary to maintain a cohesive IT environment.

In summary, the necessity test for using Microsoft Teams in a company boils down to the following: while alternative methods and tools exist for each individual function Teams offers, the platform's integrated nature and seamless connection to other widely-used Microsoft products make it necessary for businesses prioritising efficiency, cohesion, and streamlined operations.

3 | Balancing Test

The balancing test requires weighing our organisation's legitimate interests against the individual's (in this case, employees') interests, rights, and freedoms. The purpose is to determine if the business interests might unduly infringe on individual privacy rights.

3.1 Nature of Data Processed

The personal data that Microsoft Teams processes typically includes employee names, email addresses, job roles, messages exchanged, and any documents or files shared. The electronic communication is largely of a professional nature. It is however not excluded that employees will use it for personal reasons, and any personal use of Microsoft Teams should be regulated by internal policies on acceptable use so that employees are

aware of what the organisation's expectations are in this regard.

3.1.1 Assessment

The data is largely of a professional nature and is similar to what would be processed in an ordinary office environment. The risks to individual privacy from processing such personal data for communication purposes are relatively low, especially when compared to more sensitive types of personal data.

3.2 Expectation of Processing

In a modern employment relationship, employees would reasonably expect their data to be processed in this way.

3.2.1 Assessment

Given that Microsoft Teams was introduced as a broadly available and extensively used tool for communication and collaboration, employees would reasonably expect the platform to process their professional data. During the COVID-19 pandemic, the tool served as a critical cornerstone in the IT infrastructure of most organisations globally. As such, employees have come to expect the tool as a central part of collaboration and employment. As long as personal conversations or non-work-related data aren't monitored, the expectation aligns with work-related processing.

3.3 Intrusiveness and Potential Impact

The data processing part of using Microsoft Teams is not considered intrusive, and while the potential negative impact on individuals, if their data were misused or breached, could be significant, it is not considered likely.

3.3.1 Assessment

Microsoft Teams, when used as intended, doesn't delve into highly personal or sensitive areas of an individual's life. The potential harm from a breach would be concerning but is less severe than if more sensitive data were exposed. However, any misuse or unauthorised monitoring of personal conversations could be highly intrusive, highlighting the need for clear usage policies.

3.4 Pre-existing Relationship

The pre-existence of the relationship between the data subject (employee) and the data controller (employer) makes it clear to the data subject, that certain processing activities will be required to maintain the relationship.

3.4.1 Assessment

Employees have a pre-existing relationship with their employer. They expect certain tools to be

used for the purpose of their job role. This pre-existing relationship means that some level of data processing is inherently expected, further tipping the balance in favor of the legitimate interest.

3.5 Safeguards and Consent

A number of safeguards have been put in place to protect individual rights.

3.5.1 Assessment

Microsoft Teams has robust security measures in place. If additional layers of consent are incorporated (e.g., for recording meetings), and if employees are adequately informed and trained about data processing and their rights, the balance is more favorable towards the organization's interests.

Given the professional nature of the data and the context in which Microsoft Teams is used, along with appropriate safeguards, the legitimate interests of using Microsoft Teams for business purposes likely outweigh the potential risks to individual rights and freedoms. However, transparency, proper policies and guidelines, and robust security measures are crucial in ensuring this balance is maintained, cf. below.

4 | Potential Risks to Data Subjects Related to the Use of Microsoft Teams

4.1 Unauthorised Access and Data Breaches

Like any online platform, Microsoft Teams could be vulnerable to hacking attempts, potentially leading to unauthorised access to personal data, discussions, files, and other sensitive content.

Misconfigured permissions could allow unauthorised users to access private chats or team channels.

4.2 Data Retention and Deletion

Microsoft Teams retains data for specific periods, and if not correctly managed, this could lead to unnecessarily prolonged storage of personal data, violating the GDPR's data minimisation principle.

Accidental deletion of data from Teams could result in loss of vital personal or business information.

4.3 Data Transfer Outside the EU

Microsoft may store or process Teams data on servers outside the European Union. Although Microsoft complies with international data trans-

fer mechanisms, transferring data outside the EU is always considered a risk.

4.4 Third-party App Integrations

Microsoft Teams allows integration with third-party apps. If these apps have vulnerabilities or are not GDPR compliant, it could pose a risk to data subjects' privacy.

4.5 Profile Building and Analytics

Microsoft might use the data for analytics, profiling, or improving its services. This could lead to potential privacy concerns if not adequately communicated and managed.

4.6 Eavesdropping and Surveillance

Unauthorised users or malicious actors could potentially eavesdrop on video meetings or calls, leading to privacy breaches.

4.7 Lack of Awareness Among Users

Users might not be aware of all privacy settings or best practices, leading to unintended sharing of personal or sensitive data.

5 | Mitigation

By implementing robust safeguards which address the risks above, we can ensure that the legitimate interests pursued do not infringe on individual privacy rights.

5.1 Data Encryption

Protecting data both when it's being transferred (in transit) and when it's stored (at rest).

5.1.1 Measures

Ensure that all communication and data within Microsoft Teams are encrypted using industry-standard methods. This includes chat messages, shared documents, and video calls.

5.2 Access Controls

Limiting who can access what information to ensure only relevant personnel can see specific data.

5.2.1 Measures

Implement strict user roles and permissions within Microsoft Teams. For instance, administrative rights should be limited to the absolute minimum. Role-based access ensures that employees can only access the channels and data pertinent to their job functions.

5.3 Regular Review of Permissions

Ongoing checks to ensure that access permissions remain appropriate and that no unnecessary accesses are granted.

5.3.1 Measures

Schedule periodic audits of user roles and permissions within Microsoft Teams. As employees' roles change or they leave our organisation, their access rights should be adjusted or revoked accordingly.

5.4 Employee Awareness and Training

Ensuring that all staff members understand the proper use of Microsoft Teams and the importance of data protection.

5.4.1 Measures

Organise regular training sessions on Microsoft Teams, emphasising the importance of not sharing sensitive personal data unnecessarily and highlighting features like private chats versus public channels. Adopt and make employees

aware of the acceptable use policy. Additionally, educate them on phishing threats or other potential security risks associated with online communication tools.

5.5 Compliance with Microsoft's Best Practices

Microsoft provides guidelines and best practices for using Microsoft Teams in a secure manner.

5.5.1 Measures

Ensure that our organisation's setup and usage of Microsoft Teams align with Microsoft's recommended security measures. This might include using multi-factor authentication, regular software updates, and utilizing advanced security features offered by Microsoft.

5.6 Data Retention Policies

Determine how long data should be kept within Microsoft Teams in order to minimise the risk of over-retention and aged data being unnecessarily exposed.

5.6.1 Measures

Establish a clear data retention policy that aligns with business needs and regulatory requirements. This might involve automatically deleting chat histories after a certain period or archiving old files to more secure storage.

5.7 Incident Response Plan

Having a plan in place in case there's a security breach or any misuse of the platform.

5.7.1 Measures

Create a clear incident response protocol detailing the steps to take if there's a suspicion of a data breach. This plan should include immediate actions, communication strategies, and any necessary notifications to regulatory bodies or affected individuals.



6 | Review

6.1 Frequency

It is imperative that this LIA is not seen as a one-time activity. Regularly scheduled reviews, for instance, annually, should be set. However, certain triggers might necessitate earlier reviews.

6.2 Triggers for Review

6.2.1 Technological Changes

If Microsoft Teams introduces significant new features or alters how personal data is stored, shared or otherwise processed, it's crucial to re-assess whether the LIA still stands valid.

6.2.2 Organisational Changes

If our organisation undergoes structural changes, mergers, or introduces new departments or ways of working, the original conditions under which the LIA was made might change. For example, if our organisation grows and adds more teams globally, data transfer mechanisms and considerations need to be revisited.

6.2.3 Feedback and Incidents

Any feedback from employees about privacy concerns, and actual or potential data breaches related to Microsoft Teams should instigate a review of the LIA.

6.2.4 Legal and Regulatory Changes

If there are amendments to data protection laws, enforcement activities or new guidance from data protection authorities about electronic communication tools, a review would be necessary.

6.3 Review Process:

6.3.1 Stakeholder Involvement

Engage key stakeholders in the review process. This would typically involve IT for technical details, HR for employee feedback, and potentially legal for regulatory insights.

6.3.2 Revisit Original Assumptions

Re-evaluate the necessity and balancing tests. Consider if the original legitimate interests still apply, if processing the personal data is still necessary in the way it's being done, and if the balance still leans in favor of the organization rather than infringing upon individual rights.

6.3.3 Re-assess Mitigation Measures

Determine if the original mitigation measures are still effective. Perhaps there are now better encryption techniques, stricter access controls, or new features in Microsoft Teams that offer improved data protection which can be adopted.

6.3.4 Document Changes

Any changes or updates to the original LIA should be thoroughly documented. This not only ensures compliance but also demonstrates proactive accountability.

6.3.5 Feedback Loop

After the review, it's beneficial to communicate any significant changes or reaffirmations of the current practices to employees. This keeps them informed and may also alleviate any concerns regarding their data privacy.

The regular review process ensures that our organisation's use of Microsoft Teams remains

compliant with GDPR and that employees' rights and freedoms are consistently respected. It also signals to regulators and employees that our organisation is proactive and diligent about data protection.

7 | Transparency

7.1 Purpose and Implementation

Transparency ensures that employees are not only aware of the data processing activities related to using Microsoft Teams but also understand the reasons for such processing. This enables employees to make informed decisions about their data and exercise their rights, if necessary.

7.2 Communication Channels

7.2.1 Internal Communication

Use internal newsletters, emails, and team meetings to announce the introduction and usage of Microsoft Teams. This ensures that every employee, regardless of their department or position, is informed.

7.2.2 Training Sessions

Hold training sessions on how to use Microsoft Teams. These sessions should include segments on the kind of data Microsoft Teams collects and processes, and how employees can manage their data.

7.2.3 Dedicated Portal/Intranet Page

Create a dedicated section on our organisation intranet where employees can find detailed information about Microsoft Teams, its data processing activities, and FAQs related to data privacy.

7.3 Content of Communication:

7.3.1 Nature of Data Processed

Clearly outline the types of data that Microsoft Teams will process. This might include chat logs, shared documents, call recordings, and attendance logs for meetings.

7.3.2 Purpose of Processing

Explain why this data is being processed. For instance, chat logs might be stored to maintain a record of official communications, and attendance logs could be used for accountability and review purposes.

7.3.3 Duration of Storage

Inform employees about how long their data will be stored on Microsoft Teams and any backup or archival systems.

7.3.4 Third-party Sharing

If any data is being shared with third parties (e.g., external consultants using Microsoft Teams for collaborative projects), this needs to be explicitly mentioned. The purpose of such sharing and the data protection measures in place should also be communicated.

7.3.5 Individual Rights

Ensure that employees are aware of their individ-

ual rights under GDPR, such as the right to access their data, the right to rectification, and the right to object. Provide clear instructions on how they can exercise these rights. Make sure that the personal data processed by means of Microsoft Teams is discoverable for you to be able to respond to individuals' requests in an appropriate and timely manner.

7.4 Privacy Notice Update

It's essential to update our organisation's privacy notice to include using Microsoft Teams.

The updated privacy notice should be easily accessible, for instance, through a prominent link on our organisation's intranet or a notification in the email footer.

Within the notice, provide detailed information about the data processing activities related to Microsoft Teams. This can be a dedicated section or subsection that covers all the points mentioned above.

By emphasising transparency in this manner, our organisation not only complies with GDPR but also fosters trust among its employees, which is essential for the smooth and ethical operation of any organisation.



8 Conclusion

As demonstrated above, the processing of personal data by means of Microsoft Teams is carried out for specific, clear, and justifiable purposes, and it is strictly necessary to achieve legitimate objectives of organisations that use this communication and collaboration tool.

On that basis, and subject to the implementation of necessary controls/risk mitigating measures, **the outcome of the legitimate interest assessment is that processing of personal data in the context of the use of Microsoft Teams shall be considered lawful under the GDPR.**

Contact

hello@whitelabelconsultancy.com

+45 71 74 74 54

NORWAY

Main Office Oslo

 +47 4141 2168

 Fjordalléen 16
0250 Oslo

DENMARK

Copenhagen Office

 +45 71 74 74 65

 Dampfærgevej 27
2100 København Ø

POLAND

Warsaw Office

 +48 515 07 99 77

 Ul. Marszałkowska 58/15
00-545 Warszawa

UNITED ARAB EMIRATES

Dubai Office

 +971 50 4536616

 Dubai World Trade Center
Dubai

[WHITELABELCONSULTANCY.COM](https://whitelabelconsultancy.com)



Internal Use of Microsoft Teams

DECEMBER 2023

