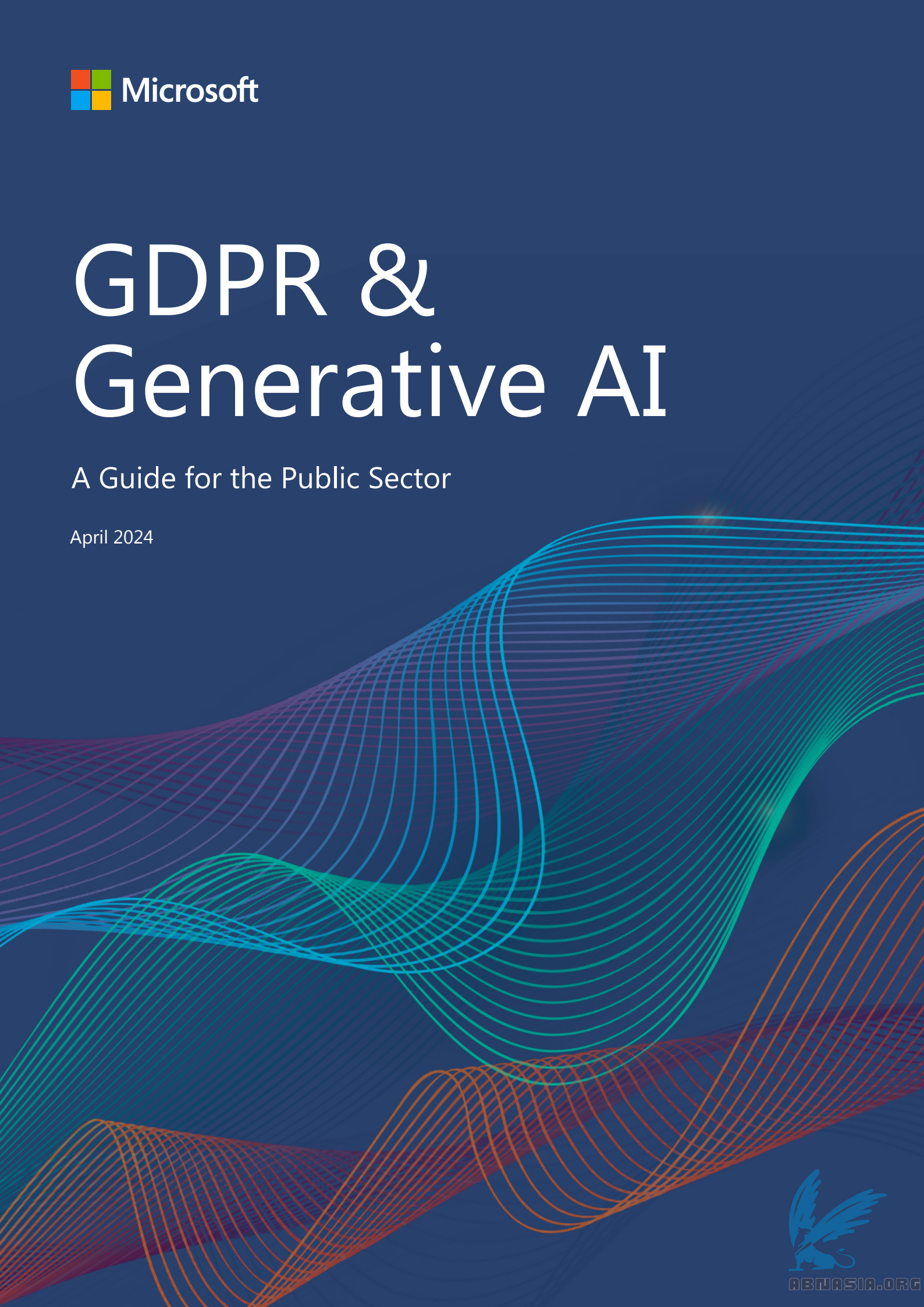
Microsoft

GDPR & Generative AI

A Guide for the Public Sector

April 2024



Contents

Executive Summary

- The use cases for generative AI in the public sector present an exciting opportunity to improve the quality and efficiency of public services. At Microsoft we want to empower our customers to harness the full potential of new technologies like generative artificial intelligence (generative AI), while complying with their obligations under the General Data Protection Regulation (GDPR).

- Microsoft is committed to ensuring its AI systems are developed responsibly and in a way that is worthy of people's trust. We drive this commitment according to six key principles which align closely with public sector priorities and the fundamental principles set out in Article 5 of the GDPR.

- When considering GDPR compliance in the context of the procurement and use of generative AI services, the fundamental principles of the GDPR apply in the same manner as they do for processing personal data in any other context (e.g. the use of cloud services). So, while AI technology may be new, the principles and accordingly the processes for risk assessment and compliance with the GDPR remain the same. Hence, to ensure GDPR compliance, public sector organizations should be confident to approach Microsoft's AI services in the same way as they have approached procuring other cloud services.

- Microsoft's existing privacy commitments including those provided in Microsoft's Data Protection Addendum extend to our AI commercial products. Public sector customers can rest assured that the privacy commitments they have long relied on when using our enterprise cloud products also apply to Copilot for Microsoft 365 and the Azure OpenAI Service. Public sector customers can therefore be confident that their valuable data is safeguarded by industry-leading data governance and privacy practices in the most trusted cloud on the market today.

- There are a number of key obligations under the GDPR which public sector organizations need to consider when procuring generative AI services. In this paper we have included details of these obligations and the associated support and resources which Microsoft can offer including in relation to international transfers of personal data, transparency, data subject rights, processor obligations, technical and organizational security measures, and DPIAs.

- Our customers' data belongs to our customers. Microsoft does not claim ownership of any customer prompts or output content created by Microsoft's generative AI solutions. In addition, no Customer Data (including prompts or output content) is used to train foundation models without customer permission.

- As the regulatory landscape evolves and we innovate to provide new kinds of AI solutions, Microsoft will continue to offer industry-leading tools, resources and support to demonstrate our enduring commitment to meeting the needs and demands of our European public sector customers in their AI journey.

Introduction

As technologies evolve, so too do the ways in which public sector organizations can embrace digital transformation technologies to help deliver on their responsibilities. It is clear that governments need to accelerate their digital and technological capabilities to meet citizen demands, while operating with often constrained budgets. Citizens increasingly expect faster, more personalised services, with an experience similar to those made available by the private sector. In response, government departments are motivated to take advantage of the efficiencies seen in other industries that have been realized by harnessing the potential of digital transformation technologies.

Effective public service delivery is both a responsibility and an opportunity for governments. Ultimately it means working efficiently with the resources available, delivering great outcomes for society, while safeguarding people's privacy and wellbeing. Getting this balance "right", requires an understanding of the best tools available, used in a responsible and secure manner, particularly given the need to safeguard personal information.

It is in this context that generative AI presents an exciting opportunity for governments. If integrated in a considered manner which safeguards personal information, AI has the potential to reduce administrative workload, increase efficiency of services, help public servants make better, faster decisions, all while increasing civil servant satisfaction and much more.

At Microsoft we want to empower our customers to harness the full potential of new technologies like generative AI, while complying with their obligations under the GDPR to ensure the privacy and security of citizens' and public institutions' data.

We have a long-standing practice of protecting our customers' information. Our approach to Responsible AI is built on a foundation of privacy, and we remain dedicated to upholding core values of privacy, security, and safety in all our generative AI products and solutions. As the use of AI solutions expands, our customers can be confident that their valuable data is safeguarded by industry-leading data governance and privacy practices in one of the most trusted clouds on the market today. Public sector customers can rest assured that the privacy commitments they have long relied on when using our enterprise cloud products also apply to our enterprise generative AI solutions that are backed by the Microsoft's Data Protection Addendum, including Copilot for Microsoft 365 and Azure OpenAI Service.

As an industry and thought leader in AI, we have developed this paper to address specific concerns relating to the GDPR-compliant use of Copilot for Microsoft 365 and the Azure OpenAI Service for public sector organizations in Europe, and to demonstrate how our AI solutions can be embraced in a GDPR-compliant manner.

This paper is set out as follows:

Part 1

Examines the meaning of responsible AI in the public sector context, the six key principles and our approach to responsible AI that guides Microsoft's development of AI products, and demonstrates the tools and resources Microsoft offers to assist your AI deployment.

Part 2

Shifts focus to the structure and requirements of the GDPR and how Microsoft can support public sector customers to embrace our AI solutions while continuing to meet their compliance obligations under the GDPR.

Parts 3 and 4

Are dedicated to an in-depth exploration of Copilot for Microsoft 365 and the Azure OpenAI Service, and how these services can be utilized in compliance with the GDPR.

Part 5

Concludes the paper, reflecting on the insights shared and the future trajectory of AI for the public sector.

Appendix 1

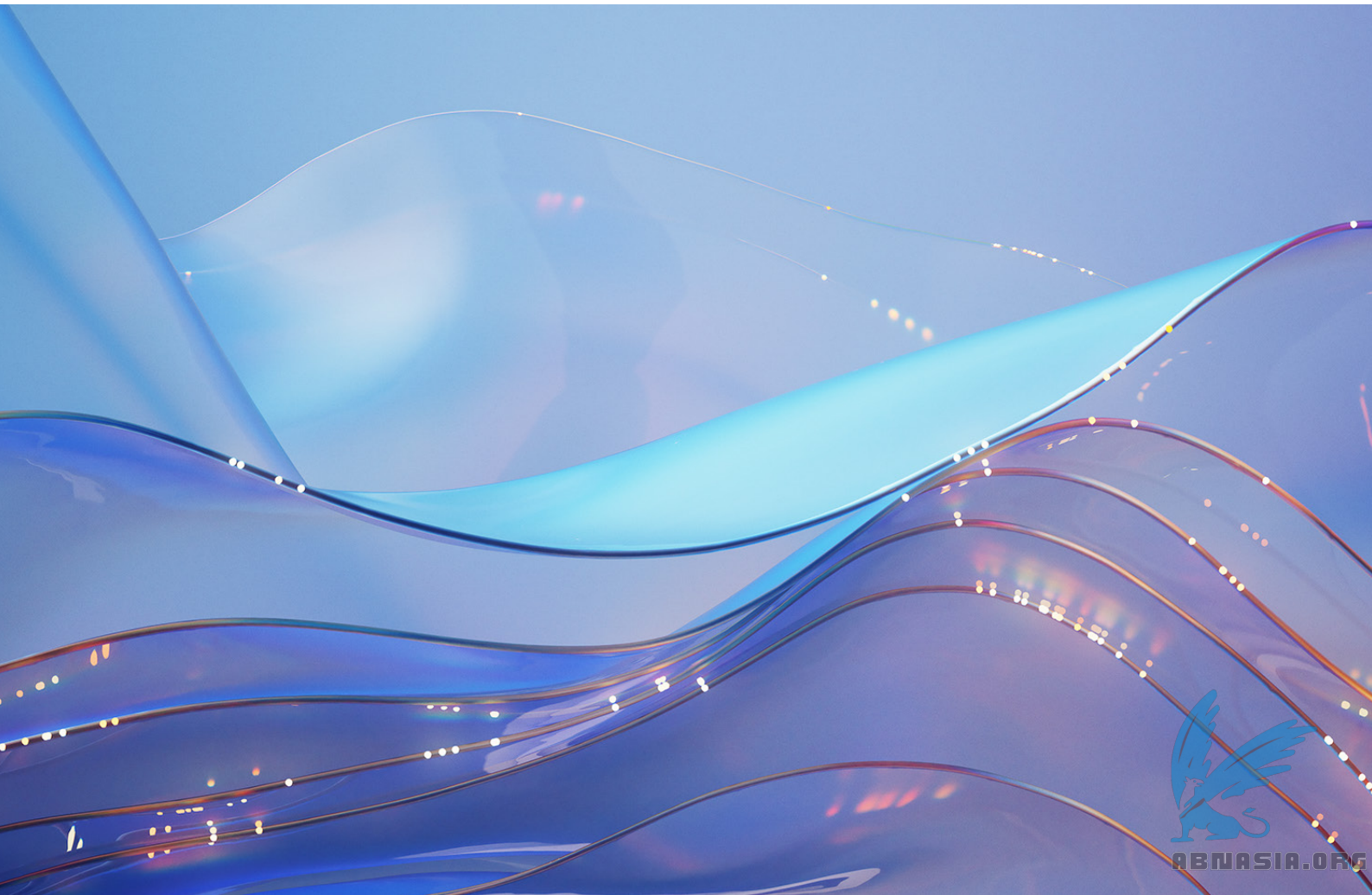
Showcases some of the exciting opportunities that generative AI presents for the public sector.

Appendix 2

Addresses some frequently asked questions (FAQs) that public sector organizations have, in relation to embracing AI in a GDPR-compliant manner.

Appendix 3

Provides links to additional resources which public sector customers can reference to supplement and expand their understanding of the information provided in this paper.



Part 1:

Responsibly using AI in the Public Sector -
Microsoft's AI journey and leveraging our tools and resources

Responsible AI in the Public Sector

AI has the potential to transform the public sector, from improving healthcare and education to enhancing public safety and transportation. The growing interest in generative AI is clear. However, with this 'great power comes great responsibility', and it is therefore essential that AI is developed and deployed responsibly. Microsoft has taken a principled role in this area with the development of comprehensive AI responsibility policies and tools, grounded on work we have been doing for many years.

The responsible use of AI is, of course, a topic which public sector organizations around the world have actively addressed in recent years. Through leading discussions, developing approaches and strategies, and implementing these in their operations, the use of AI to responsibly deliver more effective and inclusive public services is on the rise.

Learn more about Governing AI

At Microsoft, we are committed to making sure AI systems are developed responsibly and in a way that is worthy of people's trust. We drive this commitment according to **six key principles** which align closely with public sector priorities and the fundamental principles set out in **Article 5 of the GDPR:**

- **Fairness:** AI systems should be designed to treat all individuals fairly, without bias or discrimination.
- **Reliability and safety:** AI systems should be reliable and safe, with built-in mechanisms to prevent errors and minimize harm.
- **Accountability:** The creators of AI tools and the developers who leverage them should be accountable for their systems.
- **Privacy and security:** AI systems should respect individuals' privacy and data security.
- **Inclusiveness:** AI systems should be designed to be accessible and usable by everyone, including individuals with disabilities.
- **Transparency:** AI systems should be transparent and explainable, with clear documentation of their functionality and decision-making processes.

These principles can be used by public sector organizations to evaluate AI systems and processes in use or under consideration in the context of the GDPR, as explored in Part 2 below. Within Microsoft, we have established our Office of Responsible AI, which sets AI governance policies for the entire company, advises our senior leadership team on AI issues, enables engineering and compliance teams across the company to build according to responsible AI principles, all while ensuring that as a corporation we are continuing to examine and improve our ethical stance as new capabilities and challenges arise.

Learn more about Microsoft's principles and approach to Responsible AI

In June 2022, we published our internal Microsoft Responsible AI Standard for product development to share what we've learned so far in the form of concrete and actionable guidelines. We believe that industry, academia, civil society, and government need to collaborate to advance the state-of-the-art and learn from one another.

Public sector organizations should develop and be governed by responsible AI strategies, and these strategies should incorporate principles, practices, tools, and governance to enable those across the organization to assess, adopt, and manage their use of AI.

When potential risks are understood and carefully managed, the public sector can realize the promise of AI. Forward-looking leaders will ensure that their commitment to responsible AI is not an afterthought but is baked into their organization's innovation pipeline. This allows the public sector to harness the power of AI to improve the services they provide and benefit society as a whole. You can find several exciting examples of how to use generative AI in the public sector in Appendix 1.

Tools, Commitments, and Resources to Assist your AI Deployment

To support our customers and empower their compliant use of AI, Microsoft offers a range of solutions, tooling, and resources to assist in their AI deployment. From comprehensive transparency documentation to a suite of tools for data governance, risk, and compliance assessment. Dedicated programs such as our industry-leading AI Assurance Program and AI Customer Commitments further broaden the support we offer public sector customers in addressing their needs.

Microsoft's AI Assurance Program helps customers ensure that the AI applications they deploy on our platforms meet the legal and regulatory requirements for responsible AI. The program includes support for regulatory engagement and advocacy, risk framework implementation and the creation of a customer council.

For decades we've defended our customers against intellectual property claims relating to our products. Building on our previous AI Customer Commitments, Microsoft announced our Customer Copyright Commitment, which extends our intellectual property indemnity support to both Copilot for Microsoft 365 and our Azure OpenAI Service. Now, if a third party sues a customer for copyright infringement for using Copilot for Microsoft 365 or the Azure OpenAI Service, or for the output they generate, we will defend the customer and pay the amount of any adverse judgments or settlements that result from the lawsuit, as long as the customer has used the guardrails and content filters we have built into our products.

Microsoft has also developed a range of solutions to support our customers with data governance, with Microsoft Purview. You can find further detail on how Microsoft Purview can support compliance with GDPR in Part 2.

Part 2:

The GDPR Compliance Framework in the Context of AI

What is the GDPR and who does it apply to?

The General Data Protection Regulation also known as the "GDPR"[1] sets an important bar globally for privacy rights, information security, and compliance. At Microsoft, we value privacy as a fundamental right, and we believe that the GDPR plays an important role in protecting and enabling the privacy rights of individuals.

Microsoft is committed to its own compliance with the GDPR, and providing an array of products, features, documentation, and resources to support our customers in meeting their compliance obligations under the GDPR.

The GDPR is in force in the UK and all EU countries and imposes a set of data protection rules on the processing of personal data, with the goal to protect the fundamental rights of data subjects and create a level playing field for the processing of personal data and further the internal market.

Any public sector organization that processes the personal data of data subjects residing in Europe is subject to the GDPR.[2] The national laws also incorporate data protection rules and guidelines. These are generally adapted to meet and/or exceed the requirements of the GDPR.

Leverage established principles to comply with regulatory frameworks when using AI solutions

When we think about the GDPR in the context of leveraging generative AI and taking advantage of the opportunities presented by this technology, the starting point is that the fundamental principles of the GDPR still apply in the same manner as they do for processing personal data in any other context, including when using the cloud. So, while the AI technology may be new, the principles and accordingly the processes for risk assessment and compliance with the GDPR remain the same.

It is also helpful to recognize that the GDPR was drafted to be technology-agnostic and does therefore not prevent public sector organizations from embracing opportunities to use generative AI.

As such, applying established GDPR assessment processes is a great way for public sector organizations to harness the revolutionary potential of AI and deliver great outcomes for society, while safeguarding people's privacy and wellbeing. Microsoft has a long-standing history of collaborating with and assisting public sector organizations in pursuit of their digital transformation priorities while complying with the requirements of the GDPR, including in relation to the transition from on-premises to cloud computing. Public sector organizations can approach Microsoft's generative AI solutions by leveraging the approach they have used in procuring our cloud services.

Cloud computing is essential for accessing the potentially groundbreaking AI technology, and the hyper-scale cloud is, therefore, the foundation for deploying AI. Azure's enterprise-grade protections which form part of Copilot for Microsoft 365 and the Azure OpenAI Service provide a strong foundation upon which public sector customers can build their data privacy, security, and compliance systems to confidently scale AI while managing risk and ensuring compliance with the GDPR.

[1] For the purpose of this paper any references to the EU GDPR also apply to the UK GDPR.
[2] With the exceptions of EU institutions that are subject to similar rules under Regulation (EU) 2018/1725 (EUDPR) and UK institutions that are subject to similar rules under Parts 4, 5 and 7 of the Data Protection Act 2018.

Who is responsible for GDPR compliance when using AI and cloud services?

Under the GDPR, there are two key parties each with a separate set of compliance responsibilities:

- **The Data Controller:** The data controller decides why and how personal data is processed and is the entity that is the principal subject of the obligations imposed by the GDPR. Many of these obligations apply from the moment this entity starts to collect personal data about individuals.
- **The Data Processor:** In contrast, under the GDPR, the data processor is essentially a subcontractor to the data controller, processing personal data on behalf of and upon instruction from the data controller.

Public sector organizations can act as data controllers and data processors in the GDPR context. When using Microsoft's generative AI services, Microsoft's Product Terms indicate whether Microsoft is providing an Online Service as a data processor or a data controller. Most of the Online Services, including generative AI services, are provided by Microsoft as a data processor and are governed by the Data Protection Addendum. For further details on specific products and services consult the Microsoft Product Terms.

Compliance with the GDPR is a shared responsibility

GDPR compliance is a shared responsibility. Microsoft is committed to complying with all laws and regulations which are applicable to Microsoft and its generative AI tools and services including the GDPR.

As a public sector organization, you will need to determine how these tools and services will be used and what personal data will be processed to enable you to ensure you are using such tools in a complaint manner.

To assist you with that, we have designed our generative AI tools and services with privacy and data protection in mind and provide our public sector customers with information, features, and contractual commitments to support you in your compliance and accountability obligations under the GDPR. The following sections in this Part 2 delve into this in more detail and provide you with information to support your assessment of the use of Microsoft's generative AI tools and services in compliance with the GDPR.

How does Microsoft support customers with their GDPR compliance obligations?

As more public sector organizations wish to leverage generative AI, many are looking to Microsoft not only as a service provider, but as a trusted partner on the journey to helping them to meet their compliance obligations under the GDPR.

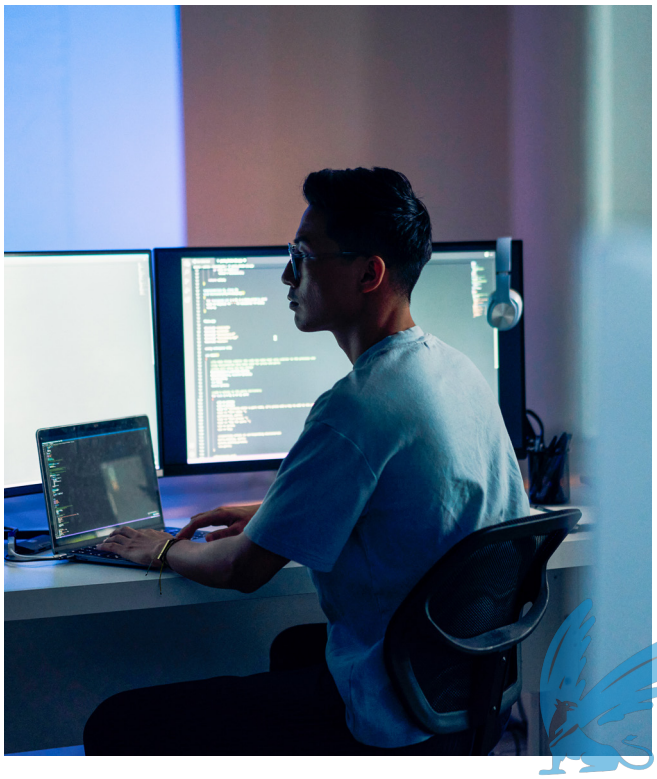
The first step towards compliance is understanding how Microsoft's generative AI services work including how they process personal data. Our comprehensive transparency documentation and information help you understand how our AI tools work and what choices our customers can make to influence system performance and behavior.

In Part 3 and Part 4 of this paper we provide specific information and links to additional resources which you can use to help enhance your understanding of these products and services.

Jump to Part 3 to find out more about Copilot for Microsoft 365

Jump to Part 4 to find out more about the Azure OpenAI Service

This knowledge provides the foundation for compliance with a number of key obligations under the GDPR. We will explore these key obligations and the associated support that Microsoft offers customers later in this Part 2 but first we will address the seven core privacy commitments which Microsoft offers to its customers in the AI era.



Protecting the data of our public sector customers - Microsoft's privacy commitments in the AI era

Microsoft's existing privacy commitments extend to our AI commercial products, as explained in a blog post from our Chief Privacy Officer Julie Brill. You can rest assured that the privacy commitments you have long relied on when using our enterprise cloud products also apply to our enterprise generative AI solutions that are backed by Microsoft's Data Protection Addendum, including Copilot for Microsoft 365 and Azure OpenAI Service.

The following seven commitments apply to "Customer Data", which is defined in Microsoft's Product Terms as all data, including all text, sound, video, or image files, and software, that are provided to Microsoft by, or on behalf of, our customers through use of an online service. All inputs (including prompts)[3] and output content[4] are Customer Data. In accordance with Microsoft's Data Protection Addendum the customer "retains all right, title and interest in and to Customer Data".

1. We will keep your organization's data private.

Your data remains private when using Copilot for Microsoft 365 and Azure OpenAI Service and is governed by our applicable privacy and contractual commitments, including the commitments we make in Microsoft's Data Protection Addendum and Microsoft's Product Terms.

2. You are in control of your organization's data.

Your data is not used in undisclosed ways or without your permission. You may choose to customize your use of Copilot for Microsoft 365 or Azure OpenAI Service, opting to use your data to fine tune models for your organization's own use. If you do use your organization's data to fine tune, any fine-tuned AI solutions created with your organization's data will be available only to you.

3. Your access control and enterprise policies are maintained.

To protect privacy within your organization when using enterprise products with generative AI capabilities, your existing permissions and access controls will continue to apply to ensure that your organization's data is displayed only to those users to whom you have given appropriate permissions.

4. Your organization's data is not shared.

Microsoft does not share your data with third parties without your permission. Your data, including the data generated through your organization's use of Copilot for Microsoft 365 or Azure OpenAI Service – such as prompts and responses – are kept private and are not disclosed to third parties.

5. Your organization's data privacy and security are protected by design.

Security and privacy are incorporated through all phases of design and implementation of Copilot for Microsoft 365 and Azure OpenAI Service. As with all our products, we provide a strong privacy and security baseline and make available additional protections that you can choose to enable. As external threats evolve, we will continue to advance our solutions and offerings to ensure world-class privacy and security in Copilot for Microsoft 365 and Azure OpenAI Service, and we will continue to be transparent about our approach.

6. Your organization's data is not used to train foundation models.

Microsoft's generative AI solutions, including Copilot for Microsoft 365 and Azure OpenAI Service capabilities, do not use Customer Data to train foundation models without your permission. Your data is never available to OpenAI or used to improve OpenAI models.

7. Our products and solutions comply with global data protection regulations.

The Microsoft AI products and solutions you deploy are compliant with today's global data protection and privacy regulations. As we continue to navigate the future of AI together, including the implementation of the EU AI Act and other global laws, organizations can be certain that Microsoft will be transparent about our privacy, safety, and security practices. We will comply with global laws that govern AI, and back up our promises with clear contractual commitments.

You can find additional details about how Microsoft's privacy commitments apply to Azure OpenAI and Copilot for Microsoft 365 here and the FAQ: Protecting the Data of our Commercial and Public Sector Customers in the AI Era.

[3] "Inputs" means all Customer Data that the customer provides, designates, selects, or inputs for use by a generative artificial intelligence technology to generate or customize an output including any customer prompts.
[4] "Output Content" means any data, text, sound, video, image, code, or other content generated by a model in response to Input.

Key obligations under the GDPR in the context of the procurement and use of generative AI services

There are a number of obligations under the GDPR which public sector organizations need to consider when procuring generative AI services. This section considers some of the key obligations and what associated support and resources Microsoft can offer to your organization to help you comply.

Articles 12 to 14 of the GDPR (Transparency)

Articles 12 to 14 of the GDPR require data controllers to provide data subjects with certain key information about how their personal data will be used. This information must be provided in a concise, transparent, intelligible, and easily accessible form, using clear and plain language. This information is often provided in the form of a privacy notice. If you deploy a new technology (such as Copilot for Microsoft 365 or Azure OpenAI Service) and intend to use such technology in a way that is not reflected in your existing privacy notices, then you will need to update your privacy notices to reflect these new processing activities.

How we help you comply: The information set out in this paper and available in our transparency resources noted below is intended to assist your understanding of how Copilot for Microsoft 365 and Azure OpenAI Service process data and the extent to which additional information (if any) needs to be communicated to data subjects. Additional product-specific information is available at Data, Privacy and Security for Azure OpenAI Service; Data, Privacy and Security for Microsoft Copilot for Microsoft 365; Copilot in Dynamics 365 and Power Platform; and FAQs for Copilot data security and privacy for Dynamics 365 and Power Platform.

Articles 15 to 21 of the GDPR (Data Subject Rights)

Under the GDPR, data controllers must ensure they are in a position to comply with their obligation to respond to requests from data subjects relating to the exercise of their rights under Articles 15 to 21 of the GDPR, with appropriate assistance from data processors where necessary.

How we help you comply: In the "Data Subjects Rights; Assistance with Requests" section of Microsoft's Data Protection Addendum, Microsoft commits to make available to customers (in a manner consistent with the functionality of the services and Microsoft's role as a data processor) the ability to fulfil requests from data subjects exercising their rights under the GDPR.

If Microsoft receives such a request directly from a data subject in situations where it is processing personal data on behalf of your organization, it will redirect the data subject to submit its request to your organization instead. You are responsible for responding to any such requests, but Microsoft will comply with reasonable assistance requests in this respect.

Microsoft has developed additional solutions to assist its customers when responding to data subject rights requests, such as Microsoft Purview and Purview eDiscovery. The features of these products empower our customers to proactively govern their AI usage and adhere to evolving regulatory requirements. This can be valuable for instance to improve efficiency in responding to and actioning requests in relation to the "right to access personal data" and the "right to be forgotten" that apply under Articles 15 and 17 of the GDPR.

Learn more about Microsoft Purview and its features and how these tools can assist you in the deployment of Microsoft's generative AI solutions

Article 28 of the GDPR (Processor Obligations)

The GDPR requires that where a public sector organization acts as a data controller that they only use data processors to process personal data on their behalf where they provide sufficient guarantees to meet key requirements of the GDPR. These key requirements are described in Article 28 of the GDPR and include that data processors commit to:

- only use subprocessors with the consent of the data controller and remain liable for subprocessors;
- process personal data only on instructions from the data controller, including with regard to transfers;
- ensure that persons who process personal data are committed to confidentiality;
- implement appropriate technical and organizational measures to ensure a level of personal data security appropriate to the risk;
- assist the data controller in its obligations to respond to data subjects' requests to exercise their GDPR rights;
- meet the GDPR's breach notification and assistance requirements;
- assist the data controller with data protection impact assessments and consultation with supervisory authorities;
- delete or return personal data at the end of provision of services; and
- support the data controller with evidence of compliance with the GDPR.

How we help you comply: Microsoft provides the contractual commitments required of data processors in Article 28 of the GDPR to its customers in Microsoft's Data Protection Addendum (DPA). You can find these specific commitments in the attachment to the DPA labelled "European Union General Data Protection Regulation Terms", in addition to the main body of the DPA addressing in detail the substantive requirements under the GDPR, including under Article 28.

In this context, it is important to emphasise that the GDPR does not require data controllers to create and use their own data protection terms with their data processors. The European Data Protection Board (EDPB) itself recognises that it is compliant to use a cloud provider's standard terms, subject to their compliance with the GDPR, and Article 28.[5]

A hyperscale cloud provider serves all of its customers uniformly. The contractual structure must accurately reflect how the processor's services operate and protect personal data. Uniformity is standard in cloud services and makes cloud services more manageable, scalable, secure, and affordable than on-site solutions. In a multi-tenant service, a change imposed by one customer may affect all customers using the service. This can be problematic if customers have inconsistent or mutually exclusive requirements. In addition, introducing different security measures or standards for different customers may undermine the security of Microsoft's services as a whole. It is therefore not feasible for Microsoft to change its operational processes or create bespoke contractual commitments and/or contractual structure for individual customers.

In light of this, public sector organizations need to understand that creating their own data processing terms when working with hyperscale cloud providers may prevent them from leveraging the rich innovation of cloud based generative AI services.

[5] Edpb_guidelines_2020-07_controllerprocessor_en.pdf (europa.eu).

Article 32 of the GDPR (Technical and Organizational Security Measures)

Article 32 of the GDPR requires data controllers and data processors to implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk taking into account the nature, scope, context and purposes of the processing of personal data. These measures should address the risks associated with accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

How we help you comply: In the "Data Security" section of the Microsoft's Data Protection Addendum, Microsoft contractually commits to implement and maintain appropriate technical and organizational measures to protect "Customer Data" and "Personal Data" against accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, such data transmitted, stored or otherwise processed.

Those technical measures are set forth in Microsoft's Security Policy and comply with ISO 27001, ISO 27002 and ISO 27018. Microsoft also contractually commits to encrypting 'Customer Data' (including any 'Personal Data' contained therein), in transit (including between Microsoft data centers) and at rest. Appendix A – Security Measures to Microsoft's Data Protection Addendum also contains comprehensive commitments from Microsoft regarding the security of 'Customer Data', including in relation to the Organization of Information Security, Asset Management, Human Resources Security, Physical and Environmental Security, Communications and Operations Management, Information Security, Incident Management and Business Continuity Management.

The technical, organizational, and security measures described above apply to any Customer Data that customers provide or create when using Copilot for Microsoft 365 and Azure OpenAI Service. You can refer to the information set out above to demonstrate the commitment and measures taken by Microsoft to protect Customer Data (including personal data).

Jump to Part 3 to find out more about Security for Copilot for Microsoft 365

Jump to Part 4 to find out more about Security for Azure OpenAI Service

Article 35 of the GDPR (Data Protection Impact Assessments)

Article 35 of the GDPR requires data controllers to undertake a data privacy impact assessment (DPIA) when processing personal data is likely to result in a high risk to the rights and freedoms of data subjects (particularly when this involves using new technologies).

When assessing whether a DPIA is required data controllers need to take into account the nature, scope, content and purposes of the processing. Therefore, whether a DPIA is required for the use of Copilot for Microsoft 365 and Azure OpenAI Service will depend on the particular use case and type of personal data which you wish to process using these services.

Learn more about when a DPIA must be completed

Even if it is not legally required, a DPIA is good practice and can help you work through the specific data protection risks associated with the implementation of Copilot for Microsoft 365 and/or Azure OpenAI Service for a specific use case. Preparing a DPIA may also assist you in meeting your accountability obligations under Article 5(2) of the GDPR.

A DPIA must contain at least:

> **(a)** a systematic description of the envisaged processing operations and the purposes of the processing;
>
> **(b)** an assessment of the necessity and proportionality of the processing operations in relation to the purposes;
>
> **(c)** an assessment of the risks to the rights and freedoms of data subjects; and
>
> **(d)** the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with the GDPR, taking into account the rights and legitimate interests of data subjects and other persons concerned.

Learn more about the contents of a DPIA

How we help you comply: The information contained in this paper and the additional resources to which it refers can assist you with completing a DPIA. In particular, the information in:

- **Part 3** and **Part 4** relating to how Copilot for Microsoft 365 and Azure OpenAI Service process data will assist with completing the elements described in (a) above; and
- the sections on technical and organizational measures for both Copilot for Microsoft 365 and Azure OpenAI Service will assist with completing the elements described in (d) above.

The assessments described in (b) and (c) will vary on a case-by-case basis depending on the use case and the nature, scope and content of the personal data involved and will need to be undertaken by you.

Learn more about Data Protection Impact Assessments for the GDPR

Articles 44 to 50 of the GDPR (Transfers of Personal Data to Third Countries)

The GDPR permits personal data to be transferred to a third country outside of the EU or EEA (including the US) where certain conditions have been satisfied. These conditions include where there has been an adequacy decision by the European Commission or where appropriate additional safeguards (such as the EU Standard Contractual Clauses) have been put in place.

For public sector customers in the UK, the UK GDPR permits personal data to be transferred to a third country outside of the UK (including the US) where certain conditions have been satisfied. These conditions include where there has been an adequacy decision by the UK Secretary of State or where appropriate additional safeguards (such as the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses ("UK Addendum") have been put in place.

How we help you comply: All transfers of personal data by Microsoft outside of the UK, EU or EEA will be subject to a valid transfer mechanism under the GDPR, including transfers to the US.

The EU Commission and the UK Secretary of State have announced adequacy decisions finding that (for the purpose of Article 45 of the GDPR) the US ensures an appropriate level of protection for personal data transferred from the UK or EU to organizations in the US that are certified to the EU-U.S. Data Privacy Framework. Microsoft is certified under the EU-U.S. Data Privacy Framework and the commitments they entail. Microsoft is committed to embracing the framework and will go beyond it by meeting or exceeding all the requirements this framework outlines for our customers.

Microsoft also continues to utilize the EU Standard Contractual Clauses and UK Addendum globally where appropriate for transfers from the UK, EU or onward transfers – to the benefit of our customers and their legal certainty around transfers that originate in the EU.

In addition to Microsoft's compliant data transfer mechanisms, Microsoft has established the EU Data Boundary making robust commitments to store and process customer's data within the EU as specified in Microsoft's Data Protection Addendum and the Microsoft Product Terms, reducing transfers of personal data to third countries thereby simplifying GDPR compliance for transfers to third countries. Both Copilot for Microsoft 365 and Azure OpenAI Services are EU Data Boundary services.

The EU Data Boundary is a geographically defined boundary (consisting of the countries in the EU and the European Free Trade Association) within which Microsoft has committed to store and process Customer Data (including any personal data) for certain enterprise online services. The EU Data Boundary uses or may use Microsoft datacenters announced or currently operating in Austria, Belgium, Denmark, Finland, France, Germany, Greece, Ireland, Italy, Netherlands, Norway, Poland, Spain, Sweden, and Switzerland. In the future, Microsoft may establish datacenters in additional countries located in the EU or EFTA to provide EU Data Boundary Services.

There are limited exceptions to the EU Data Boundary that may result in Microsoft processing Customer Data (including personal data) outside of the EU Data Boundary. Where this is the case, Microsoft relies on compliant data transfer mechanisms as set out in the GDPR. Further details relating to these limited circumstances can be found in the Microsoft Product Terms.

Learn more about the EU Data Boundary

Jump to Part 3 to find out more about Data Residency for Copilot for Microsoft 365

Jump to Part 4 to find out more about Data Residency for Azure OpenAI service

How does the GDPR interact with the AI Act ?

The GDPR and the AI Act are intended to be complementary and operate alongside each other providing a regulatory framework for AI products and services. The GDPR, which regulates the processing of personal data by controllers and data processors, focuses on data privacy and aims to give individuals control over their personal data.

The AI Act, which applies to providers, importers, distributers, users, and others involved in the AI lifecycle, aims to ensure that AI systems that are used in the EU respect fundamental rights, safety, and ethical principles, as well as address certain risks related to the most highly capable general-purpose AI models.

Find out more about the AI Act and its interaction with the GDPR in the Appendix 2: Frequently Asked Questions (FAQs).

Our continued compliance with data protection regulation and open dialogue with key regulators in Europe and across the globe

As privacy and data protection laws advance, norms and requirements evolve in Europe and across the globe; you can be certain that Microsoft will be transparent about our privacy, safety, and security practices. We will comply with laws in Europe and globally that govern AI, and back up our promises with clear contractual commitments.

Beyond adhering to the GDPR and other regulatory requirements applicable to us, Microsoft prioritizes an open dialogue with its customers, partners, and regulatory authorities to better understand and address evolving privacy and data protection concerns.

We continue to work closely with data protection authorities and privacy regulators around the world to share information about how our AI systems work thereby fostering an environment of trust and cooperation.

Part 3:

Copilot for Microsoft 365

Understanding the potential of generative AI services and how these products and services operate and use personal data is the foundation for compliance with a number of obligations under the GDPR. This Part 3 provides information and links to various external resources which can help you understand how Copilot for Microsoft 365 operates and provides key information about the product and its features which can be used to assist with completion of a DPIA or other data protection assessment/analysis.

What is Copilot for Microsoft 365 and how does it work?

Copilot for Microsoft 365 is an AI-powered productivity tool that uses "Large Language Models (LLMs)" to work alongside popular Microsoft 365 apps such as Word, Excel, PowerPoint, Outlook, Teams, and more. Copilot for Microsoft 365 provides real-time, intelligent assistance which enables users to enhance their creativity, productivity, and skills.

Copilot for Microsoft 365 is built on top of the same cloud infrastructure as its Microsoft 365 applications, and applies the same principles of confidentiality and privacy to Customer Data that Microsoft has leveraged for years. Copilot for Microsoft 365 adheres to all existing privacy, security, and compliance commitments that apply to Microsoft 365 including Microsoft's GDPR commitments as set out in Microsoft's Data Protection Addendum and in relation to the EU Data Boundary.

Copilot for Microsoft 365 uses the organizational content in your Microsoft 365 tenant, including users' calendars, emails, chats, documents, meetings, contacts, and more only in accordance with existing access permissions. The richness of the Copilot for Microsoft 365 experience depends on the data sources indexed by Microsoft 365. Customers with the most abundant data in Microsoft 365 (Exchange, OneDrive, SharePoint, Teams) will get the best results from Copilot. With access to comprehensive organizational data, Copilot can suggest more relevant and personalised content based on the user's work context and preferences.

Copilot responds to prompts from your users. A "prompt" is the term used to describe how you ask Copilot for Microsoft 365 to do something for you — such as creating, summarising, editing, or transforming. Think about prompting like having a conversation, using plain but clear language and providing context like you would with an assistant.

When Copilot for Microsoft 365 uses content from the organization's Microsoft 365 tenant to augment the user's prompt and enrich the response, as described above, this is called "grounding". Grounding is different to training. No Customer Data is being used to train the LLM. In fact, the LLM is stateless, meaning that it retains no information about the prompt that was submitted to it, nor any Customer Data that was used to ground it, nor any responses it provided.

Copilot for Microsoft 365 leverages an instance of a foundation LLM hosted in Azure OpenAI. Copilot for Microsoft 365 does not interact with any services operated by OpenAI (e.g. ChatGPT, or the OpenAI API). OpenAI is not a sub-processor to Microsoft and Customer Data - including the data generated through your organization's use of Copilot for Microsoft 365 such as prompts and responses – are not shared with third parties without your permission.

To get the best responses and the most out of Copilot for Microsoft 365, it's important that you input suitable prompts and avoid certain common pitfalls. Learn more about the skill of prompting: the art and science of prompting (the ingredients of a prompt) and prompting do's and don'ts.

Copilot for Microsoft 365 is:

- **Built** on Microsoft's comprehensive approach to security, compliance, and privacy;
- **Designed** to protect tenant, group, and individual data; and
- **Committed** to responsible AI.

Get an inside look at how LLMs work when you use them with your data in Microsoft 365. Learn more about Copilot for Microsoft 365.

Learn about how Copilot can be used in your favourite Microsoft apps by visiting the Copilot Lab.

You can also find more detailed information about Copilot for Microsoft 365 in our Learn portal.

Copilot and your privacy

Copilot in Windows

Learn more about how Copilot uses your data to assist you on your Windows device.

Learn more about your data and privacy

Copilot Pro (home users)

Learn more about how Copilot uses your data in Microsoft 365 apps at home.

Read about Microsoft 365 apps and your privacy

Copilot for Microsoft 365 (IT Pros/admins)

Learn more about how your organizational data is used and protected when using Copilot with Microsoft 365.

Get details about data, privacy, and security

How does Copilot for Microsoft 365 use personal data?

Copilot for Microsoft 365 provides value by connecting Microsoft's LLMs to your organizational data. Copilot for Microsoft 365 accesses content and context to generate responses anchored in your organizational data, such as user documents, emails, calendar, chats, meetings, and contacts. Copilot for Microsoft 365 combines this content with the user's working context, such as the meeting a user is currently attending, email exchanges the user had on a topic, or chat conversations the user had in a given period. Copilot for Microsoft 365 uses this combination of content and context to help provide accurate, relevant, and contextual responses to the user's prompts.
Copilot for Microsoft 365 can reference web content from the Bing search index to ground user prompts and responses. Based on the user's prompt, Copilot for Microsoft 365 determines whether it needs to use Bing to query web content to help provide a relevant response to the user. Controls are available to manage the use of web content for admins.

Abuse monitoring for Copilot for Microsoft 365 occurs in real-time, without providing Microsoft any standing access to Customer Data, either for human or for automated review. While abuse moderation, which includes human review of content, is available for Azure OpenAI Service, this is not required for Copilot for Microsoft 365.

Microsoft will collect and store data about user interactions with Copilot for Microsoft 365. This will include the user's prompt, how Copilot responded, and the information used to ground Copilot's response ("Content Interactions"). Customer admins can view, manage, and search your organization's Content Interactions. It may be necessary to update your privacy notices for your organization's users to ensure it appropriately captures any processing of personal data by admins in this context. See Part 2 for further details of the transparency obligations under the GDPR.

It is important for Microsoft that our customers' data belongs to our customers. Microsoft does not claim ownership of the content created by Copilot for Microsoft 365. All Content Interactions including user prompts and any output data/content qualifies as "Customer Data" in our Product Terms and Microsoft's Data Protection Addendum.

All Customer Data processed by Copilot for Microsoft 365 is processed and stored in alignment with contractual commitments with your organization's other content in Microsoft 365.

Copilot for Microsoft 365 does not use Customer Data to train foundation models without the customers' permission.

Security for Copilot for Microsoft 365

As noted in Part 2, the GDPR requires data controllers and data processors to implement appropriate technical and organizational measures to ensure a level of security for any personal data which they process.

The same security and compliance terms apply, by default, to Copilot for Microsoft 365 as already apply for your organization's use of Microsoft 365. Copilot for Microsoft 365 is hosted in Azure infrastructure and protected by some of the most comprehensive enterprise compliance and security controls in the industry. Copilot for Microsoft 365 was built to take advantage of the security and compliance features that are already well-established in Microsoft's hyperscale cloud. This includes prioritization of reliability, redundancy, availability, and scalability, all of which are designed into our cloud services by default.

Copilot for Microsoft 365 also respects each user's access permissions to any content that it retrieves. This is important because Copilot for Microsoft 365 will only generate responses based on information the particular user has permission to access.

Microsoft already implements multiple forms of protection to help prevent customers from compromising Microsoft 365 services and applications or gaining unauthorized access to other tenants or the Microsoft 365 system itself.

Below are a few examples of those forms of protection:

- Logical isolation of Customer Data within each tenant for Microsoft 365 services is achieved through Microsoft Entra authorization and role-based access control. Learn more about Microsoft 365 isolation controls.
- Microsoft uses rigorous physical security, background screening, and a multi-layered encryption strategy to protect the confidentiality and integrity of Customer Data.
- Microsoft 365 uses service-side technologies that encrypt Customer Data both at rest and in transit, including BitLocker, per-file encryption, Transport Layer Security (TLS), and Internet Protocol Security (Ipsec). Learn more about encryption in Microsoft 365, see Encryption in the Microsoft Cloud.
- Your control over your organization's data is reinforced by Microsoft's commitment to comply with broadly applicable privacy laws including the GDPR and privacy standards, such as ISO/IEC 27018, the world's first international code of practice for cloud privacy.
- For content accessed through Copilot for Microsoft 365 plug-ins, encryption can exclude programmatic access, thus limiting the plug-in from accessing the content. Learn more about Configure usage rights for Azure Information Protection.
- As generative AI systems are also software systems, all elements of our Security Development Lifecycle apply: from threat modeling to static analysis, secure build and operations, use of strong cryptography, identity standards, and more.
- We've also added new steps to our Security Development Lifecycle to prepare for AI threat vectors, including updating the Threat Modeling SDL requirement to account for AI and machine learning-specific threats. We put our AI products through AI red teaming to look for vulnerabilities and ensure we have proper mitigation strategies in place.

Learn more about Data, Privacy, and Security for Copilot for Microsoft 365

EU Data Boundary and Data Residency

As we explained in Part 2 of this paper, Copilot for Microsoft 365 is an EU Data Boundary Service.

Learn more about the EU Data Boundary

When you store data generated by Copilot for Microsoft 365 in Microsoft 365 products that already have data residency commitments under the Product Terms, then the applicable commitments will be upheld.

Copilot for Microsoft 365 has been added as a covered workload in the data residency commitments in the Microsoft Product Terms. Microsoft Advanced Data Residency (ADR) and Multi-Geo Capabilities offerings also include data residency commitments for Copilot for Microsoft 365 customers.

Part 4:

Azure OpenAI Service

Understanding how generative AI products and services operate and use personal data is the foundation for compliance with a number of obligations under the GDPR. This Part 4 provides information and links to various external resources which can help you understand how Azure OpenAI Service operates and provides key information about the service and its features which can be used to assist with completion of a DPIA or other data protection assessment/analysis.

What is Azure OpenAI Service and how does it work?

Azure OpenAI Service is a cloud-based platform that enables customers to build and deploy their own generative AI applications leveraging the power of AI models. Azure OpenAI Service provides customers with access to a set of LLMs for the development of generative AI experiences.

From generating realistic images and videos to enhancing customer experiences, generative AI has proven to be a versatile tool across various industries. The models underlying Azure OpenAI Service can be easily adapted to your specific task including: content design, creation and generation; summarization; semantic search; natural language to code translation; accelerated automation; personalised marketing; chatbots and virtual assistants; product and service innovation; language translation and natural language processing; fraud detection and cybersecurity; predictive analytics and forecasting; creative writing; and medical research and diagnosis.

Azure OpenAI Service is fully controlled by Microsoft. Microsoft hosts the OpenAI/Chat GPT models in Microsoft's Azure environment and the service does not interact with any services operated by OpenAI (e.g. ChatGPT or the OpenAI API).

OpenAI/ChatGPT owns and trains the foundation LLMs which Microsoft uses, and Microsoft has a license to offer services that rely on these foundation LLMs.

OpenAI/ChatGPT is not a sub-processor to Microsoft and customer data - including the data generated through your organization's use of Azure OpenAI Service– such as prompts and responses – are kept private and are not shared with third parties without your permission.

Learn more about the underlying LLMs that power the Azure OpenAI Service

Azure OpenAI Service can be used in the following ways:

- **Prompt engineering:** Prompt engineering is a technique that involves designing prompts for LLMs. Prompts are submitted by the user, and content is generated by the service, via the completions, chat completions, images, and embeddings operations. This process improves the accuracy and relevance of responses, optimizing the performance of the model.

  Learn more about prompt engineering

- **Azure OpenAI On Your Data:** When using the "on your data" feature, the service retrieves relevant data from a configured Customer Data store and augments the prompt to produce generations that are grounded with your data.

  Azure OpenAI "on your data" enables you to run supported LLMs on your organization's data without needing to train or fine-tune models. Running models on Customer Data enables you to analyze your data with greater accuracy and speed. By doing so, you can unlock valuable insights that can help you make better decisions, identify trends and patterns, and optimize your operations.

  One of the key benefits of Azure OpenAI "on your data" is its ability to tailor the content of conversational AI. The model within Azure OpenAI Service has access to and can reference specific sources to support responses, answers are not only based on its pre-trained knowledge but also on the latest information available in the designated data source. This grounding data also helps the model to avoid generating responses based on outdated or incorrect information.

  Learn more about Azure OpenAI On Your Data

- **Azure OpenAI fine-tuning:** You can provide your own training data consisting of prompt-completion pairs for the purposes of fine-tuning an OpenAI model. This process finetunes an existing LLM using example data. This fine-tuning refers to the process of retraining pre-trained models on specific datasets, typically to improve model performance on specific tasks or introduce information that wasn't well represented when the base model was originally trained. The outcome is a new "custom" LLM that has been optimized for the customer using the provided examples.

  Training data and fine-tuned models:

  1. Are available exclusively for use by your organization.
  2. Are stored within the same region as the Azure OpenAI resource.
  3. Can be deleted by the customer at any time.

  When you upload custom data to fine tune the results of the LLM, both the Customer Data and the results of the fine-tuned model are maintained in a protected area of the cloud, stored in your tenant – accessible only by your organization and separated by robust controls to prevent any other access. The Customer Data and results can additionally be encrypted by either Microsoft-managed or customer-managed encryption keys in a Bring Your Own Key format if a customer so chooses.

  In most instances, Microsoft can support and troubleshoot any problems with the service without needing access to any Customer Data (such as the data that was uploaded for fine-tuning). In the rare cases where access to Customer Data is required, whether it be in response to a customer-initiated support ticket or a problem identified by Microsoft, you can assert control over access to that data by using Customer Lockbox for Microsoft Azure. Customer Lockbox gives customers the ability to approve or reject any access request to their Customer Data.

  Learn more about Azure OpenAI fine tuning

Whether content is used to ground prompts using the "on your own data" feature, or whether content is used to build a fine-tuning model, the Customer Data is not being used to train the foundation LLM. In fact, the LLM is stateless, meaning that it retains no information about the prompt that was submitted to it, nor any Customer Data that was used to ground it, nor any responses it provided. The LLM is not trained and does not learn at any point during this process, it is exactly the same foundational model even after millions of prompts are run through it.

You can find detailed information about Azure OpenAI Services through the Azure OpenAI Service - Documentation, quickstarts and API reference guides

Preventing abuse and harmful content generation

To reduce the risk of harmful use of Azure OpenAI Service, both content filtering and abuse monitoring features are included.

Content filtering is the process by which responses are synchronously examined by automated means to determine if they should be filtered before being returned to a user. This examination happens without the need to store any data, and with no human review of the prompts (i.e. the text provided by users as requests) or the responses (i.e. the data delivered back to the user.)

Learn more about content filtering

Abuse monitoring is conducted by a separate process. This data may be accessed only by authorized Microsoft personnel to assist with debugging, and protect against abuse or misuse of the system. The human reviewers are authorized Microsoft employees who access the data via point wise queries using request IDs, Secure Access Workstations (SAWs), and Just-In-Time (JIT) request approval granted by team managers.

Learn more about abuse monitoring

This human review may create a challenge for public sector customers, who need to strike a balance between the safety of the system and the risks of external access – even under controlled conditions. To accommodate that balance, Microsoft offers limited access features that allow for approved customer-use cases to opt out of these human review and data logging processes.

Some customers may want to use Azure OpenAI Service for a use case that involves the processing of sensitive, highly confidential, or legally regulated input data but where the likelihood of harmful outputs and/or misuse is low. These customers may conclude that they do not want or do not have the right to permit Microsoft to process such data for abuse detection, as described above, due to their internal policies or applicable law. To address these concerns, Microsoft allows customers who meet additional Limited Access eligibility criteria and attest to specific use cases to apply to disable the Azure OpenAI content management features by completing this form.

If Microsoft approves a customer's request to disable abuse monitoring, then Microsoft does not store any prompts and completions associated with the approved Azure subscription for which abuse monitoring is configured off. In this case, because no prompts and completions are stored at rest in the service results store, the human review process is not possible and is not performed.

How does the Azure OpenAI Service use personal data?

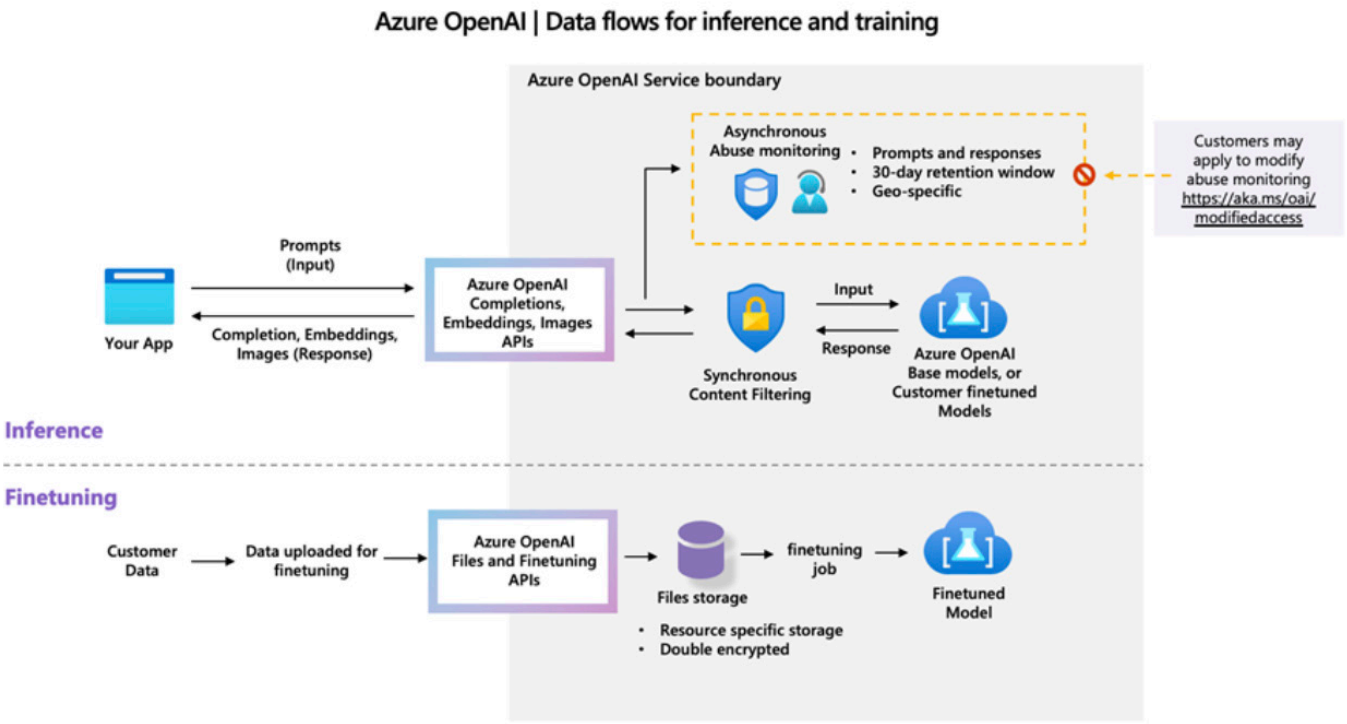
The diagram below illustrates how your organization's data is processed by Azure OpenAI Service. This diagram covers three different types of processing:

1. How Azure OpenAI Service processes your prompts to **generate content** (including when additional data from a connected data source is added to a prompt using Azure OpenAI "On Your Data").
2. How Azure OpenAI Service **creates a fine-tuned (custom) model** with your training data.
3. How Azure OpenAI Service and Microsoft personnel **analyze** prompts, completions, and images for harmful content and for patterns suggesting the use of the service in a manner that violates the Code of Conduct or other applicable product terms.

Customer prompts (inputs) and completions (outputs), embeddings, and training data:

- are NOT available **to other customers**.
- are NOT available **to OpenAI**.
- are NOT used **to train foundation models** without the customer's permission.
- are NOT used **to improve any Microsoft or 3rd party products or services**.
- are NOT used **for automatically improving Azure OpenAI models** for your use in your resource (the models are stateless unless you explicitly fine-tune models with your training data).

Customer fine-tuned Azure OpenAI models are available exclusively for your organization's use.



Security for Azure OpenAI

As noted in Part 2 of this paper, the GDPR requires data controllers and data processors to implement appropriate technical and organizational measures to ensure a level of security for any personal data which they process.

Security is built-in throughout the development lifecycle of all of our enterprise services (including those that include generative AI technology), from inception to deployment.

Azure OpenAI Service is hosted in Azure infrastructure and protected by some of the most comprehensive enterprise compliance and security controls in the industry. These services were built to take advantage of the security and compliance features that are already well-established in Microsoft's hyperscale cloud. This includes prioritization of reliability, redundancy, availability, and scalability, all of which are designed into our cloud services by default.

As generative AI systems are also software systems, all elements of our Security Development Lifecycle apply: from threat modelling to static analysis, secure build and operations, use of strong cryptography, identity standards, and more.

We've also added new steps to our Security Development Lifecycle to prepare for AI threat vectors, including updating the Threat Modelling SDL requirement to account for AI and machine learning-specific threats. We put our AI products through AI red teaming to look for vulnerabilities and confirm we have proper mitigation strategies in place.

Learn more about data, privacy and security for Azure OpenAI Service

EU Data Boundary and Data Residency

Azure OpenAI Service is an EU Data Boundary service. For the purpose of interpreting the "EU Data Boundary Services" section of the Product Terms, Azure OpenAI service is an Azure service that enables deployment in a region within the EU Data Boundary.

Learn more about the EU Data Boundary

In relation to:

- **Azure OpenAI on your Data feature:** Any data sources you provide to ground the generated results remain stored in the data source and location you designate. No data is copied into Azure OpenAI service.
- **Training data and fine-tuned (custom) LLMs:** These are stored within the same region as Azure OpenAI resource in the customer's Azure tenant.
- **Abuse monitoring for customers who use Azure OpenAI Service in Europe:** This review is conducted exclusively by Microsoft employees in the European Economic Area. The data store where prompts and completions are stored is logically separated by customer resource (each request includes the resource ID of the customer's Azure OpenAI resource). A separate data store is located in each region in which Azure OpenAI service is available, and a customer's prompts and generated content are stored in the Azure region where the customer's Azure OpenAI service resource is deployed, within the Azure OpenAI service boundary.

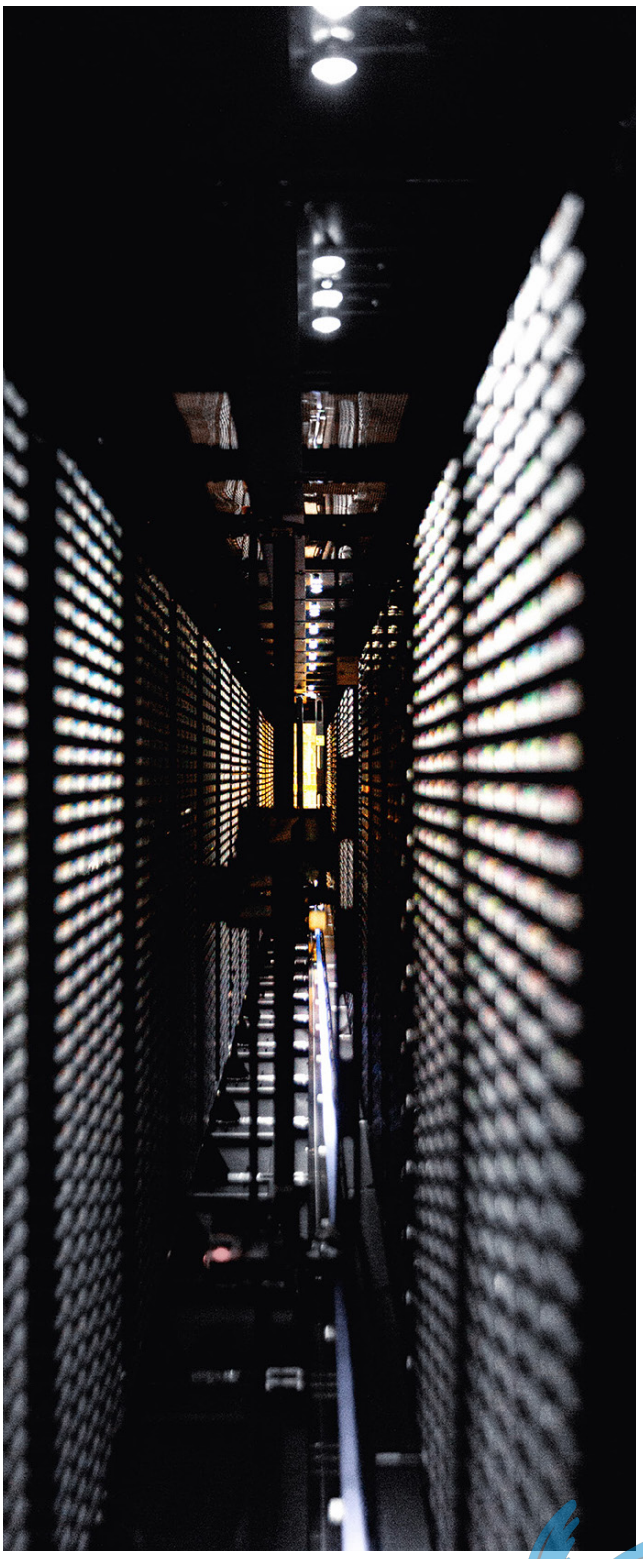
Part 5:

Conclusion

Microsoft runs on trust. We are committed to security, privacy, and compliance across everything we do, and our approach to generative AI is no different. As an industry leader in the provision of generative AI solutions we are trusted by public sector customers across the world and adhere to the strictest privacy and security standards in the industry. We provide superior products and services to our public sector customers, thereby facilitating continued progress towards national digital transformation goals.

Furthermore, we have been intentional about signalling to our public sector customers our willingness and commitment to get our data protection and privacy settings right to ensure compliance with the GDPR. We demonstrate this commitment through our contracts, extensive technical documentation (providing details about our data processes and activities), and the implementation of technical and organizational safeguards to mitigate residual privacy and security risks. This is backed by consistent engagement with regulatory and industry stakeholders whom we partner with on our journey towards responsibility, accountability, and integrity in the delivery of generative AI solutions at scale.

As the regulatory landscape evolves and we innovate to provide new kinds of AI solutions, we are keenly aware that public sector organizations will continue to look to us to help decipher and operationalize the requirements of new and existing data protection frameworks. Microsoft will continue to offer industry-leading tools, transparency resources and support and we look forward to the opportunity to continue to demonstrate our enduring commitment to meeting the needs and demands of our European public sector customers in their AI journey.



Appendix 1:

Opportunities arising from generative AI in the Public Sector

The availability of generative AI solutions has served as an accelerator to the consideration of public sector generative AI use cases. This Appendix sets out several relevant areas of impact for consideration by public sector organizations.

- **Citizen Services:** Generative AI can help governments and public sector organizations provide enhanced service experiences that make government more accessible and less time-consuming by acting as an "Information Assistant" – answering frequently asked questions, recommending services based on inputs, and even handling simple transactions.

  Many governments have already experimented with chatbots to help answer simple questions about COVID vaccinations, provide support during tax time, and offer answers to common inquiries. Generative AI helps chatbots handle more open domain questions over more sophisticated and complex materials, including rapid responses to a broader range of questions at anytime from anywhere, increasing accessibility for citizens while simultaneously increasing government efficiency and reducing administrative burden.

  Citizens can even provide a narrative of their current circumstances and discover service options they previously did not know existed. These tools also free up public sector workers to focus on strategic projects instead of being tied down to mundane, repetitive functions such as responding to common questions.

- **Internal Efficiency:** Government can be complex even for government employees! Providing public sector workers with the capacity to intuitively search and interact via chat with intranets and public sector materials in an automated fashion eases onboarding of new employees, increases efficiency between silos and departments, and minimizes administrative burdens. This capability lets public sector staff focus on their mission priorities, reducing burnout and allowing them to do more with less.

- **Deep Data:** Large language models (LLMs) can tackle the intersection between vast troves of data which may have been previously analyzed separately and manually. Simple prompts to the AI can yield both typical and unexpected connections between topics and domains that can help to spur the analytic process.

  Insightful and succinct summaries of vast amounts of media coverage or public feedback can be generated in seconds. Generative AI helps to objectively challenge conventional wisdom – raising new angles, questions, or counterarguments that may have been implicitly screened by the bias of the author. This approach ultimately yields stronger and more comprehensive output.

- **Creative Aid:** No more writer's block! Generative AI can provide helpful initial drafts of abstracts, outlines, speeches, simple correspondence, memos, frequently asked questions, whitepapers, and citizen guides. While official communications should always require a human in the loop to verify accuracy, apply human "voice," and ensure that the information is complete and not misleading, generative AI as a creative writing aid can accelerate the process dramatically and help light the creative spark while reducing time-to-completion for common writing tasks.

- **Enhance Security:** Generative AI can support cybersecurity teams and protect your organization from threats. Generative AI models can be trained to review applications and code for weaknesses using a dynamic model that evolves to keep pace with threat. This can also be used to review and deploy new code more quickly by automating vulnerability detection which will help security professional scale workloads by freeing them up from lower value tasks.

By improving citizen services, increasing efficiency, better managing and analyzing data, and serving as a creative aid, generative AI can help to create a more effective, inclusive, and responsive government.

Generative AI can also help create a more efficient, productive, and rewarding work environment for public sector employees. Governments should carefully consider the implications of using AI in their operations and take appropriate measures to ensure that the technology is used ethically and responsibly. Now is the time for public sector organizations to begin leveraging and adopting generative AI capabilities, and they can and should do so from a position of engagement and experimentation.

Appendix 2:

Frequently Asked Questions (FAQs)

How is my organization's data protected when I use Microsoft's Generative AI Services?

Microsoft runs on trust. We are committed to security, privacy, and compliance across everything we do, and our approach to generative AI is no different.

Privacy is built into our approach to Responsible AI and we will continue to uphold our core values of privacy, security, fairness, accountability, transparency, reliability, inclusiveness and safety in our AI products and solutions.

In Part 2 of this paper, we outline seven commitments that demonstrate our continued commitment to protecting our customers' data when they use our Generative AI services:

- We will keep your organization's data private.
- You are in control of your organization's data.
- Your access control and enterprise policies are maintained.
- Your organization's data is not shared without your permission.
- Your organization's data privacy and security are protected by design.
- Your organization's data is not used to train foundation models without your permission.
- Our products and solutions continue to comply with global data protection regulations.

What is generative AI and what are the different types of AI models Microsoft uses?

Generative AI is a type of artificial intelligence that can create new things, like pictures, text, or speech, that are similar to examples it has seen before. It does this by learning from a set of examples, figuring out the patterns and rules that make them similar, and then using those patterns and rules to make new examples that are similar to the ones it learned from. It's different from other types of AI because it can create new things, instead of just recognizing or classifying things it has seen before.

Microsoft's Azure OpenAI service and Copilot for Microsoft 365 allow customers to leverage OpenAI's models, including GPT-3, GPT-4, and Codex in the Microsoft environment. These models are commonly referred to as "foundation models," which are generally understood to be large-scale AI models that are trained on vast quantities of primarily unlabeled data at scale (usually by self-supervised learning), and can be adapted with minimal fine-tuning for a range of different downstream tasks.

What are the differences between procuring cloud and generative AI services from a GDPR perspective?

The obligations under the GDPR which apply to procuring and using cloud computing services are the same as those which apply to procuring and using generative AI services. The GDPR requires a risk-based approach to be taken towards the implementation and use of any new technologies.

The level of risk involved will depend on the nature, scope, content, and purpose for which personal data will be used. When procuring cloud services and/or generative AI services, a public sector organization will need to consider what technical and organizational measures are in place to protect and safeguard the use of personal data and ensure that it has appropriate contractual commitments and operational processes to ensure it can comply with its obligations under the GDPR.

Find out more about how Microsoft can assist public sector customers in undertaking this assessment when they are looking to use Copilot for Microsoft 365 and/or Azure OpenAI Service in Part 2 of this paper.

What are the key obligations of the GDPR that apply to procuring generative AI systems?

The obligations under the GDPR will apply whenever a generative AI system uses or otherwise processes personal data.

Key obligations which public sector organizations should consider when procuring and/or implementing generative AI systems include:

- consider whether you need to update your privacy notices to reflect any new processing activity or to clarify activities (Articles 12 to 14 of the GDPR);
- ensure you have processes in place to enable you to comply with data subject rights requests (Articles 15 to 21 of the GDPR);
- ensure that any agreement you have with a data processor complies with Article 28 of the GDPR including in relation to security measures and international transfers;
- consider whether you need to conduct a data protection impact assessment (DPIA) (Article 35 of the GDPR); and
- ensure that all transfers of data outside of the UK, EU or EEA are made subject to a valid transfer mechanism (Articles 44 to 50).

Learn more about how Microsoft assists public sector customers in meeting these obligations in Part 2 of this paper.

How does the GDPR interact with the AI Act?

The AI Act is a new law currently being put in place in the EU to regulate AI systems. It will apply to providers, importers, distributers, users, and others involved in the AI lifecycle, aiming to ensure that AI systems that are used in the EU respect fundamental rights, safety, and ethical principles, as well as address certain risks related to the most highly capable general-purpose AI models.

The GDPR and the AI Act are intended to be complementary and operate alongside each other providing a regulatory framework for AI products and services.

The GDPR, which regulates the processing of personal data by data controllers and data processors, focuses on data privacy and aims to give individuals control over their personal data. Under the AI Act most of the regulatory burden will fall on providers of high-risk AI systems and general-purpose AI (GPAI) models.

Although the GDPR and the AI Act are different in their scope and purpose, they interact with each other in several ways. For example:

- The GDPR requires data controllers to conduct a DPIA in certain circumstances. The AI Act refers to this obligation and requires users of high-risk AI systems to use certain mandatory user-facing information to comply with their DPIA-obligations under the GDPR.
- The GDPR applies where personal data is processed to train an AI system or where an AI system is being used to process personal data.

Adopting the measures outlined in this paper for GDPR compliance is therefore complementary to the AI Act and the associated obligations that will apply under this new legislation.

At Microsoft, we are committed to compliance with the EU AI Act. Our multi-year effort to define, evolve, and implement our Microsoft Responsible AI Standard and internal governance has strengthened our readiness. As final requirements under the EU AI Act are defined in more detail, we look forward to working with policymakers to ensure feasible implementation and application of the rules, to demonstrating our compliance, and to engaging with our customers and other stakeholders to support compliance across the ecosystem.

How does Microsoft comply with applicable law?

Microsoft's AI products and solutions are designed and built for compliance with applicable data protection and privacy laws today, including the GDPR.

Microsoft's approach to protecting privacy in AI is underpinned by a commitment to compliance with existing and emerging regulatory and legal obligations globally. We will continue to support meaningful privacy and AI regulation, and believe that the best way to make rapid progress on needed guardrails for AI is to lean in to existing legal protections, approaches and regulatory tools that could be applied to protecting privacy and safety in these systems today.

Does Microsoft share Customer Data with OpenAI/ChatGPT?

No. Your organization's Customer Data, including prompts (inputs) and completions (outputs), your embeddings, and any training data you might provide to the Microsoft Online Services are not available to OpenAI.

Azure OpenAI Service is fully controlled by Microsoft; Microsoft hosts the OpenAI models in Microsoft's Azure environment and Azure OpenAI Service does not interact with any services operated by OpenAI (e.g., ChatGPT, or the OpenAI API). OpenAI is not a sub-processor to Microsoft.

Learn more about the underlying OpenAI models that power Azure OpenAI Service.

Can I share confidential information with Microsoft's Generative AI services?

Yes. When using Azure OpenAI or Copilot for Microsoft 365, customers may confidently share their confidential information. The foundation models that are accessed via Azure OpenAI Service and Copilot for Microsoft 365 do not use Customer Data for training without permission. These foundation models are stateless and do not store any data, including prompts that a customer inputs and completions that the model outputs. Customers can also trust that their confidential information will not be transmitted to other customers.

How does Microsoft protect security in this new era of AI?

Security is built-in throughout the development lifecycle of all of our enterprise services (including those that include generative AI technology), from inception to deployment.

Azure OpenAI Service and Copilot for Microsoft 365 are hosted in Azure infrastructure and protected by some of the most comprehensive enterprise compliance and security controls in the industry. These services were built to take advantage of the security and compliance features that are already well-established in Microsoft's hyperscale cloud. This includes prioritization of reliability, redundancy, availability, and scalability, all of which are designed into our cloud services by default.

Because generative AI systems are also software systems, all elements of our Security Development Lifecycle apply: from threat modeling to static analysis, secure build and operations, use of strong cryptography, identity standards, and more. We've also added new steps to our Security Development Lifecycle to prepare for AI threat vectors, including updating the Threat Modeling SDL requirement to account for AI and machine learning-specific threats. We put our AI products through AI red teaming to look for vulnerabilities and ensure we have proper mitigation strategies in place.

Learn more about Security for Copilot for Microsoft 365 in Part 3 of this paper, and about Security for Azure OpenAI Service in Part 4 of this paper.

Are data transfers to countries outside of the UK, EU or EEA allowed under the GDPR?

Yes, personal data can be transferred to countries outside the UK, EU or EEA where certain conditions are met including where: (a) there is an adequacy decision by the European Commission or the UK Secretary of State (Article 45 of the GDPR); or (b) the transfer is subject to additional safeguards which include the EU Standard Contractual Clauses and the UK IDTA (Article 46 of the GDPR).

Microsoft's transfers of personal data outside of the UK, EU or EEA utilize valid transfer mechanisms under the GDPR, including EU-U.S. Data Privacy Framework certification and EU Standard Contractual Clauses as appropriate.

Find out more about how Microsoft approaches data transfers to third countries in Part 2 of this paper.

Where will my data be stored and processed?

Your data residency choices will be respected when you use Microsoft's Generative AI products and services that offer local storage and/or processing capabilities.

Azure OpenAI Service and Copilot for Microsoft 365 will process and store your data within EU/EFTA for EU Data Boundary (EUDB) customers, as set forth in the Product Terms and the EU Data Boundary Transparency Documentation.

Do public sector organizations need to develop a customized data protection addendum (DPA)?

No, the GDPR does not require that each data controller has a customized data protection addendum with their data processors. Microsoft's Data Protection Addendum is compliant with the requirements of Article 28 of the GDPR.

It is not viable for hyperscale cloud providers to offer different terms for different customers as it is the uniformity of the services which makes cloud services more manageable, scalable, secure and affordable than on-site solutions. In addition, introducing different security measures or standards for different customers could undermine the security of Microsoft's services as a whole. It is therefore not feasible for Microsoft to change its operational processes or create bespoke contractual commitments and/or contractual structure for every customer.

Find out more about Microsoft's data processor obligations in Part 2 of this paper.

How can public sector customers set up their procurement of generative AI services to be compliant with the GDPR?

The GDPR requires data controllers to consider data protection issues at every stage of their processing activities, from the initial design (including during the procurement phase) to final implementation.

The risks associated with the use of generative AI in the public sector will vary depending on the specific use case and related nature, sensitivity, and volume of personal data that will be used in connection with that use case.

One way you can demonstrate compliance with the GDPR is to complete a data protection impact assessment (DPIA) relating to specific use cases for generative AI solutions. A DPIA helps organizations identify and reduce the data protection risks. A DPIA is legally required where the processing activity is likely to result in a high risk to the rights and freedoms of data subjects. Even if it is not legally required, a DPIA is good practice and can help you work through the specific data protection risks associated with how you wish to implement generative AI for a specific use case.

Find out more about DPIAs in Part 2 of this paper.

Can a public sector customer comply with the GDPR when using a public cloud to use generative AI services?

Microsoft's public cloud services have been developed to ensure they can be used by public sector customers in compliance with the GDPR (and many public sector customers already make use of these services). The information set out in this paper and contained in the Product Terms and Data Protection Addendum can be used by you to undertake an appropriate risk-based assessment of any proposed use of Copilot for Microsoft 365 and Azure OpenAI Service so as to demonstrate compliance with the relevant requirements of the GDPR.

How can public sector organizations comply with their transparency obligations under the GDPR when deploying AI technologies?

Articles 12 to 14 of the GDPR require public sector organizations to provide data subjects with certain key information about how their personal data will be used. This information is often provided in the form of privacy notices. If you deploy a new technology (such as Copilot for Microsoft 365 or Azure OpenAI Service) and intend to use such technology in a way that is not reflected in your exiting privacy notices, then you will need to update their privacy notice to reflect these new processing activities.

The information set out in this paper is intended to assist you to understand how Copilot for Microsoft 365 and Azure OpenAI Service use data and to determine what information needs to be communicated to data subjects.

Appendix 3:

Additional Resources

Microsoft is committed to providing our customers with clear information about how we use and share data, and choices they have in managing their data. This Appendix sets out additional resources which you can reference to supplement and expand on the information set out in this paper.

Responsible AI

- Empowering responsible AI practices
- Governing AI: A Blueprint for the Future
- Microsoft's principles and approach to Responsible AI
- Microsoft Responsible AI Standard

Microsoft's Customer Commitments

- AI Assurance Program and AI Customer Commitments
- Customer Copyright Commitment
- Protecting the data of our commercial and public sector customers in the AI era
- FAQ: Protecting the Data of our Commercial and Public Sector Customers in the AI Era

Understanding Generative AI

- The underlying LLMs that power Microsoft's generative AI solutions
- The art and science of prompting (the ingredients of a prompt)
- Prompting do's and don'ts

Data Protection Addendum and Product Terms

- Data Protection Addendum
- Microsoft Product Terms

Data Residency Commitments

- The EU Data Boundary
- EU Data Boundary Transparency Documentation
- Advanced Data Residency (ADR)
- Multi-Geo Capabilities

Data Protection Impact Assessments (DPIA)

- DPIAs and their contents
- Data Protection Impact Assessments for the GDPR

Copilot for Microsoft 365

- Copilot for Microsoft 365
- Copilot Lab
- Copilot for Microsoft 365 Documentation
- Data, Privacy, and Security for Copilot for Microsoft 365
- FAQs for Copilot data security and privacy
- Microsoft 365 isolation controls
- Encryption in the Microsoft Cloud

Azure OpenAI Service

- Azure OpenAI Service - Documentation, quickstarts and API reference guides
- Configure usage rights for Azure Information Protection
- Data, privacy and security for Azure OpenAI Service
- Prompt Engineering
- Azure OpenAI On Your Data
- Azure OpenAI fine tuning
- Content filtering
- Abuse monitoring
- Enterprise security for Azure Machine Learning

Microsoft