TOMORIS
MORE THAN IT

FREE DOWNLOAD

TEMPLATE · TOMORIS TOOLBOX

AI Usage Policy: Template for Companies

Sample text with placeholders, legal framework under the AI Act as amended by the Digital Omnibus and the GDPR, rollout checklist

UPDATED	LENGTH	ONLINE
Oct 25, 2026	PDF, 10 pages	tomoris.com/en/downloads/ki-nutzungsrichtlinie-vorlage

AT A GLANCE

Art. 4
Promote AI literacy: mandatory for every deployer

Jul 27, 2026
Digital Omnibus on AI in force, Regulation (EU) 2026/1744

Aug 2, 2026
Transparency obligations under Art. 50 apply

Dec 2, 2027
High-risk obligations for Annex III, such as recruitment

WHO IT IS FOR

- Management that wants to regulate and take responsibility for the use of AI assistants
- Data protection officers and those responsible for data protection
- IT managers who approve and secure tools such as Microsoft Copilot (formerly Microsoft 365 Copilot), ChatGPT or Claude
- HR departments that organize training and review AI in HR processes

Adaptation for your own use permitted; redistribute unchanged

WHAT THIS COVERS

If you provide AI assistants to your employees, you are a deployer under the AI Act and must promote your staff's AI literacy; since July 27, 2026, the version of Art. 4 as amended by the Digital Omnibus applies. This document summarizes the legal framework with references and provides sample text for an internal AI usage policy: scope, approved tools, data classes, review of results, labeling, training, reporting channels and responsible persons. A checklist helps with the rollout.

This template provides an overview and does not replace legal advice. The text of the law in its current version is decisive, in particular the AI Act including Regulation (EU) 2026/1744 and the GDPR. Adapt the sample text to your company, your tools and contracts, and coordinate it internally, for example with data protection and the works council.

Usage: You may adapt this template for your own use; you may redistribute it only in unchanged form.

CONTENTS

01 What the policy is for 2
02 The legal framework in six terms 3
03 Legal status as of October 25, 2026 4
04 Sample text, part 1: scope, tools and data 5
05 Sample text, part 2: results, training and responsibility 6
06 Reviewing tools: what vendors commit to 8
07 Checklist: rolling out the policy 8
08 Common mistakes 9
09 Sources 10

01

What the policy is for

Clear rules on which AI tools are allowed, which data may be entered, who reviews results and who is responsible.

An AI usage policy defines which AI tools are allowed in the company, for what purposes, with which data and under what controls. The BSI recommends informing employees which AI applications they may use for which purposes, what inputs they may make and how they may reuse outputs. These rules should be set down in binding form, for example in a policy, and supported technically, for example by blocking or enabling certain services (BSI, Generative AI Models, version 2.0, measure M16).

The RTR AI Service Desk advises reflecting the company's approach in an internal AI policy: with clear roles, references to other policies, clearly communicated and easy for employees to find. To be able to demonstrate implementation of Art. 4 of the AI Act, it recommends recording the AI strategy, policy and training concept in writing and documenting training per person.

The AI Act does not require a written policy. For Art. 4, the European Commission requires neither a certificate nor an AI officer; companies can document training and other measures internally (AI Literacy Q&A). The policy is the tool you use to implement and demonstrate the obligations under the AI Act and the GDPR in everyday work.

02

The legal framework in six terms

Who is a deployer, what Art. 4, 5, 26 and 50 of the AI Act require and which GDPR principles apply.

AI Act (EU) 2024/1689 as amended by Regulation (EU) 2026/1744, GDPR	
Deployer	A deployer is anyone who uses an AI system under their own authority, except in the course of a personal non-professional activity (Art. 3(4)). If a company provides an AI assistant to its employees, it is a deployer. Anyone who develops an AI system or has one developed and places it on the market or puts it into service under their own name, such as a custom-built chatbot, is a provider (Art. 3(3)).
AI literacy (Art. 4)	Providers and deployers take measures to support the development of AI literacy of their staff and other persons operating and using AI systems on their behalf. Knowledge, experience, education and training, and the context of use must be taken into account. You do not have to guarantee a specific level of literacy for anyone (Art. 4(1)). The obligation applies regardless of the risk class of the system (RTR).
Prohibited practices (Art. 5)	Prohibited are, e.g., manipulative techniques that cause significant harm, social scoring and inferring emotions in the workplace and in educational institutions, except for medical or safety reasons (Art. 5(1)(a), (c) and (f)). From December 2, 2026, also AI for intimate depictions of identifiable persons without their explicit consent and for material under Directive 2011/93/EU; deployers are only prohibited from using it for this purpose (points (ba), (bb), para. 1a). Fines of up to €35 million or 7% of worldwide turnover, whichever is higher, for SMEs whichever is lower (Art. 99(3), (6)).
Transparency (Art. 50)	Deployers disclose that image, audio or video content has been artificially generated or manipulated if it is a deepfake. The same applies to AI text published to inform the public on matters of public interest, unless it has undergone human review or editorial control and someone holds editorial responsibility (Art. 50(4)). Providers of chatbots make it clear that people are interacting with an AI (para. 1). Applies since August 2, 2026.
High-risk AI (Art. 26)	Deployers of high-risk AI systems use them in accordance with the instructions for use, assign human oversight to competent persons, monitor operation, keep logs for at least six months and inform workers' representatives and affected persons before use in the workplace (Art. 26(1), (2), (5), (6) and (7)). High-risk systems include, for example, systems for selecting applicants or evaluating performance (Annex III no. 4); these obligations apply to them from December 2, 2027.

GDPR principles	You process personal data lawfully and transparently, for specified purposes, limited to what is necessary, accurately, for no longer than necessary and securely (Art. 5(1) GDPR); you must be able to demonstrate compliance (para. 2). If an AI service processes data on your behalf, you need a processor providing sufficient guarantees (Art. 28(1)). If a high risk is likely, a data protection impact assessment must be carried out in advance (Art. 35(1)).

03

Legal status as of October 25, 2026

The Digital Omnibus on AI has been in force since July 27, 2026. What it changes for deployers and which deadlines now apply.

The European Commission proposed the Digital Omnibus on AI on November 19, 2025. It was adopted as Regulation (EU) 2026/1744 of July 8, 2026, published in the Official Journal on July 24, 2026, and has been in force since July 27, 2026 (Art. 4: third day after publication).

Dates of application under Art. 113 AI Act as amended by Regulation (EU) 2026/1744

Feb 2, 2025
AI literacy, prohibitions
Chapters I and II apply: definitions, AI literacy under Art. 4 and prohibited practices under Art. 5 (Art. 113(3)(a)).

Aug 2, 2026
Transparency, supervision
General date of application, including for Art. 50. From now on, national market surveillance authorities also supervise Art. 4 (European Commission).

Dec 2, 2026
New prohibitions
Prohibitions under Art. 5(1)(ba) and (bb). By then, providers of existing systems mark AI content in a machine-readable format (Art. 111(4)).

Dec 2, 2027
High-risk under Annex III
Chapter III Sections 1 to 3, and thus Art. 26, for high-risk systems under Annex III, for example in HR (Art. 113(3)(c)).

Aug 2, 2028
High-risk under Annex I
The same obligations for high-risk systems in products under Annex I Section A, such as toys or medical devices (Art. 113(3)(c)); for Section B, such as machinery, Art. 2(2) applies.

For deployers of AI assistants, the key points are: Art. 4 no longer requires ensuring, to their best extent, a “sufficient level” of AI literacy, but rather measures that support its development (Art. 1(5) Regulation 2026/1744). Art. 5 gains two new prohibitions, and the high-risk obligations start later (Art. 1 nos. 7 and 40). Art. 26 and Art. 50(1) to (4) remained unchanged.

> Do not confuse: in parallel, the Commission also proposed amendments to the GDPR (Digital Omnibus Regulation, COM(2025) 837). According to EUR-Lex, this procedure 2025/0360/COD has not yet been completed as of October 25, 2026. The GDPR in its previous version applies.

04

Sample text, part 1: scope, tools and data

Sections 1 to 4 with Annexes 1 and 2. Replace everything in square brackets and delete what does not apply.

How to use the sample text: replace the placeholders in square brackets, fill in the annexes and coordinate the text with data protection, information security, HR and, if there is one, the works council. The RTR cites interdisciplinary monitoring by technology, legal, compliance, IT security, HR and the works council as good practice, depending on company size.

AI usage policy of [Company], version [Version] of [MM/DD/YYYY]

§ 1 Purpose and scope	This policy governs the use of AI tools at [Company]. It applies to all employees and to persons who work with AI systems on our behalf, such as [service providers, temporary workers], and to all professional use, including on private devices. AI tools are applications that generate or analyze text, images, audio, video or code, including AI features in existing software.
§ 2 Approved tools	For work, use only the tools listed in Annex 1, with the account specified there and for the purposes specified there. Private accounts and consumer versions are not permitted for company data. Request new tools and new AI features from [Unit]; approval is granted after a review of data protection, contract and security. IT may block services that have not been approved.
§ 3 Data and inputs	What you may enter depends on the data classes in Annex 2. Enter only what is necessary for the task. Enter personal data, trade secrets and confidential customer data only into tools that Annex 1 expressly approves for this. Enter health data and other special categories under Art. 9 GDPR only if [Unit] has approved the specific purpose. Never enter credentials or passwords.
§ 4 Access and autonomous actions	AI assistants with access to emails, files or other systems can find anything you yourself are allowed to see. Report overly broad sharing permissions to [IT unit]. Use features that act autonomously, such as sending emails, changing data or placing orders, only if [Unit] has approved them and you confirm each action in advance.

Annex 1: Approved AI tools (to fill in, sample row in square brackets)

TOOL AND ACCOUNT	PERMITTED PURPOSES	HIGHEST DATA CLASS	RESPONSIBLE
[e.g. Microsoft Copilot Chat with work account]	[drafts, summaries, translations]	[internal]	[Name, role]
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____

Annex 2: Data classes and what may go into which tool (adapt to your classification)

DATA CLASS	EXAMPLES	PERMITTED IN
Public	published texts, website, brochures	all tools in Annex 1
Internal	processes, templates, drafts without reference to individuals or customers	tools with a company account: [Tool]
Confidential	quotes, contracts, cost calculations, source code, trade secrets	only expressly approved tools: [Tool]
Personal	names, contact details, customer data, HR records	only tools with a data processing agreement (DPA): [Tool]
Special categories, credentials	health data and other data under Art. 9 GDPR, passwords, keys	[no tool] or only after individual approval by [Unit]; credentials never

05

Sample text, part 2: results, training and responsibility

Sections 5 to 11 with Annex 3: human review, labeling, third-party rights, training, reporting, roles, review.

§ 5 Review results

AI results can be wrong, outdated or fabricated, even if they sound convincing. Review every result before you use it, and verify facts, figures, quotes and sources. [Role] approves content with external impact before publication. Decisions about people, for example on applications, performance or termination, are made by a human; AI may at most prepare them.

§ 6 Code and configurations

Before use, check program code and configurations generated by AI, such as firewall rules or scripts, for errors, security vulnerabilities and outdated libraries. Never accept outputs without review that go directly into other applications, a command line or a browser.

§ 7 Labeling

We label AI-generated or manipulated image, audio and video content that resembles real persons, places or events and could appear authentic (deepfakes). We label AI texts that we publish to inform the public on matters of public interest, unless they have undergone human review or editorial control and [Role] holds editorial responsibility for them (Art. 50(4) AI Act). Customer chatbots identify themselves as AI. [Optional: additional voluntary labeling]

§ 8 Third-party rights and trade secrets

Upload third-party texts, images or code only if we are allowed to use them for this purpose. AI results can reproduce protected content from training data: check images and longer text passages before publication, for images for example with a reverse image search. Treat confidential information from customers and partners like your own; contractual confidentiality obligations take precedence.

§ 9 Training	Anyone who uses AI tools attends an introduction before first use and then a refresher [annually]. Content includes at least: how the tools work and their limits, typical errors such as hallucinations and bias, this policy, the tools in Annex 1 and the reporting channels. [Unit] documents per person the type, content and objective, organizer, date and repetitions.
§ 10 Report errors and incidents	Report the following to [Contact] without undue delay: data in a tool that has not been approved, faulty results with consequences, unusual behavior of a tool, such as instructions from third-party documents, and unintended actions. If personal data is affected, [Data protection] immediately assesses whether the breach must be reported to the supervisory authority: without undue delay and, where feasible, within 72 hours (Art. 33(1) GDPR).
§ 11 Responsibility, review, effective date	The roles in Annex 3 are binding. Managers ensure that their teams know the policy. [Unit] reviews the policy and Annex 1 at least [annually] and whenever there are new tools, new AI features or changes in the legal situation. This policy applies from [MM/DD/YYYY], approved by [Name, role]. [Optional: consequences of violations, agreed with HR and the works council]

Annex 3: Roles and contacts (to fill in)

ROLE	NAME, ROLE	DEPUTY
Responsible for the policy	_____	_____
Approval of new tools and AI features	_____	_____
Data protection	_____	_____
Information security	_____	_____
Training and documentation	_____	_____
Reporting point for errors and incidents	_____	_____

Why § 8 matters: under § 26b para. 1 no. 3 UWG (Austrian Unfair Competition Act), a trade secret is only protected if it is subject to reasonable confidentiality measures. Rules on which confidential information may go into which AI tools can be part of such measures.

06

Reviewing tools: what vendors commit to

Two examples from vendor documentation, as of October 25, 2026. Review every tool yourself before it goes into Annex 1.

Microsoft Copilot	This is now the name of Microsoft 365 Copilot. According to Microsoft, prompts, responses and data accessed through Microsoft Graph are not used to train the foundation models. Copilot only shows company data for which the user has at least view permission; Microsoft advises using the permission models, for example in SharePoint, for this. The EU Data Boundary applies to EU customers; Anthropic models as subprocessors are currently excluded from it (Microsoft Learn).
Claude, commercial offerings	By default, Anthropic does not use inputs and outputs from commercial products such as Claude for Work and the Anthropic API for training. Exceptions are explicitly submitted feedback, for example via the thumbs button, and other permission; feedback is stored together with the conversation for up to five years and can be turned off in Team and Enterprise plans. Consumer products such as Claude Free, Pro and Max are subject to their own rules (Anthropic Privacy Center).

Vendor information changes. Your contract and the current documentation are decisive; for other services, such as ChatGPT, their own terms apply. The BSI advises selecting tools according to defined criteria, such as features, training data, security safeguards, liability and operation (measure M1). Record in Annex 1 which account and which contract variant is approved.

07

Checklist: rolling out the policy

Fourteen steps from the initial inventory to regular review.

- [ ] Inventory: record AI systems and AI features, including in standard software and after updates (RTR).
- [ ] Clarify the role per tool: deployer or, for example with your own chatbot, provider (Art. 3(3) and (4)).
- [ ] Review purposes: nothing under Art. 5; assess Annex III purposes such as applicant selection as high-risk.
- [ ] Select tools according to criteria: features, data use, security, terms (BSI M1).
- [ ] Clarify contracts: data processing (Art. 28 GDPR), training with inputs, storage location.
- [ ] Update the record of processing activities (Art. 30 GDPR), assess the need for a data protection impact assessment (Art. 35).

- [ ] Clean up permissions before an assistant accesses SharePoint, OneDrive or Teams.
- [ ] Block services that have not been approved technically, allow approved ones selectively (BSI M16).
- [ ] Adapt the sample text, coordinate it with data protection, IT security, HR and the works council, and approve it.
- [ ] Announce the policy and store it where everyone can find it easily (RTR).
- [ ] Plan, deliver and document training per person, including for new hires (Art. 4, RTR).
- [ ] Set up a reporting channel; define who assesses a notification under Art. 33 GDPR.
- [ ] Embed labeling under Art. 50(4) in the approval process for publications.
- [ ] Review the policy and Annex 1 regularly and whenever there is cause (RTR).

> The sample text and checklist are TOMORIS recommendations. Legally required are the obligations of the AI Act and the GDPR mentioned above; neither law prescribes a specific form for the policy.

08

Common mistakes

What makes a policy ineffective and how to avoid it.

- Policy without a tool list: without Annex 1, it is unclear what is allowed.
- Overlooking AI features in existing software: updates to standard software often bring new AI components too (RTR).
- Permissions not cleaned up: Microsoft Copilot uses content a user is allowed to access, including files that are shared too broadly (Microsoft Learn).
- Accepting results without review: convincing outputs encourage automation bias (BSI R8).
- Adopting the legal status before the Digital Omnibus: since July 27, 2026, Art. 4 no longer requires a “sufficient level”; high-risk obligations under Annex III only apply from December 2, 2027.
- Forgetting data protection: if personal data reaches third parties without authorization, there may be a reportable breach (Art. 4(12) and Art. 33 GDPR).

NEXT STEP

Check It Yourself or Put It into Practice Together

DISCUSS IMPLEMENTATION

Get in Touch
tomoris.com/en/contact

contact@tomoris.com

09

Sources

All statements are supported by sources. Legislation applies in its current version.

1 **Regulation (EU) 2024/1689 (AI Act), consolidated version of July 27, 2026, EUR-Lex**
Art. 3(3) and (4); Art. 4, 5, 26, 50, 99, 111, 113; Annexes I and III; accessed October 25, 2026
eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:02024R1689-20...

2 **Regulation (EU) 2026/1744 (Digital Omnibus Regulation on AI), OJ L of July 24, 2026**
Art. 1(5), (7), (20), (39), (40) and Art. 4; accessed October 25, 2026
eur-lex.europa.eu/eli/reg/2026/1744/oj/deu

3 **EUR-Lex: procedure 2025/0360/COD, Digital Omnibus Regulation (COM(2025) 837)**
Status "Ongoing," accessed October 25, 2026
eur-lex.europa.eu/procedure/DE/2025_360

4 **Regulation (EU) 2016/679 (GDPR), EUR-Lex**
Art. 4(12), Art. 5, 9, 28, 30, 33, 35
eur-lex.europa.eu/eli/reg/2016/679/oj/deu

5 **European Commission: AI Literacy – Questions & Answers**
As of October 20, 2026, accessed October 25, 2026
digital-strategy.ec.europa.eu/en/faqs/ai-literacy-questions-ans...

6 **RTR AI Service Desk: AI literacy**
Sections on implementation, operational implementation, documentation; accessed October 25, 2026
www.rtr.at/rtr/service/ki-servicestelle/ai-act/ki-kompetenz.de....

7 **BSI: Generative AI Models – Opportunities and Risks for Industry and Authorities, version 2.0**
Version 2.0 of January 17, 2025; risks R3 to R6 and R8, measures M1, M16 to M18, M20
www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/KI/Generative_KI-Mo...

8 **Microsoft Learn: Data, privacy and security for Microsoft Copilot**
Sections on organizational data, EU Data Boundary, protection; accessed October 25, 2026
learn.microsoft.com/de-de/microsoft-365/copilot/microsoft-365-c...

9 **Anthropic Privacy Center: Is my data used for model training? (commercial products)**
As of August 18, 2026, accessed October 25, 2026
privacy.claude.com/en/articles/7996868-is-my-data-used-for-mode...

10 **Bundesgesetz gegen den unlauteren Wettbewerb (UWG, Austrian Unfair Competition Act), § 26b, RIS**
www.ris.bka.gv.at/NormDokument.wxe?Abfrage=Bundesnormen&Gesetze...