Generatieve AI

Gebruiksbeleid

Version 3.0 – June 2026
Author: Competency Center AI / LLM
Contact: AIGovBoard@smals.be

Wat is generatieve AI?

Generatieve AI, of kortweg GenAI, zijn modellen die op basis van een vraag of beschrijving nieuwe inhoud aanmaken – denk aan tekst, code, afbeeldingen of video's. Ze zijn bijzonder veelzijdig: dezelfde technologie kan een tekst schrijven, een document samenvatten, vragen beantwoorden of code genereren.

Belangrijk om te weten: deze modellen werken probabilistisch. Dat betekent dat ze niet één vaste "juiste" respons kennen: dezelfde vraag kan tot verschillende antwoorden leiden. Hun antwoorden zijn gebaseerd op patronen uit hun trainingsdata, tenzij je ze expliciet vraagt om een antwoord te baseren op een tekst die jij aanlevert.

Bekende voorbeelden zijn ChatGPT, Claude en Gemini, maar generatieve AI zit ook verwerkt in tools die je dagelijks gebruikt, zoals Microsoft Office (Copilot) of zoekmachines.

Bij Smals zijn deze tools al actief in gebruik – en ze zullen ons werk steeds meer ondersteunen. Maar ze brengen ook risico's mee: rond privacy, correctheid, bias en overmatig vertrouwen. Dit beleid geeft je concrete richtlijnen om die risico's te beperken.

De focus ligt op tools voor tekst- en codegeneratie, want die zijn het meest verspreid binnen Smals. Dit beleid zal verder evolueren naarmate de technologie en het gebruik ervan veranderen.

Toepassingsgebied

Dit beleid geldt voor intern gebruik van generatieve AI-tools bij Smals. Het gaat niet over de ontwikkeling van applicaties die generatieve AI integreren – daarvoor gelden projectspecifieke afspraken.

Regelgevend kader

Vier belangrijke Europese en Belgische regelgevingskaders vormen de basis voor dit beleid:

EU AI Act (Verordening 2024/1689): Hierin wordt een op risico's gebaseerde indeling van AI-systemen vastgelegd. Elk AI-systeem dat wordt gebruikt in het kader van openbaar bestuur, wetshandhaving of kritieke infrastructuur kan in de categorie "hoog risico" vallen, wat leidt tot verplichte eisen op het gebied van menselijk toezicht, transparantie, logboekregistratie en conformiteitsbeoordelingen.

Algemene Verordening Gegevensbescherming (AVG) / General Data Protection Regulation (GDPR): Regelt de verwerking van persoonsgegevens. Wanneer GenAI-tools persoonsgegevens verwerken, genereren of afleiden, zijn de GDPR-verplichtingen volledig van toepassing, met inbegrip van de rechtsgrondslag, transparantie, gegevensminimalisatie, doelbinding en de

rechten van de betrokkene, zoals het recht op uitleg over geautomatiseerde beslissingen. AI-gerelateerde inbreuken in verband met persoonsgegevens moeten worden gedocumenteerd en, indien vereist, binnen 72 uur worden gemeld aan de Belgische Gegevensbeschermingsautoriteit (GBA/APD), en aan de betrokkenen wanneer sprake is van een hoog risico.

CyFun (Cyber Fundamentals Framework – CCB België): Biedt een basis van cyberbeveiligingsmaatregelen die zijn gestructureerd rond vijf functies: Identificeren, Beschermen, Detecteren, Reageren en Herstellen. GenAI-tools moeten worden beoordeeld aan de hand van dit kader, met name wat betreft toegangscontrole, traceerbaarheid, incidentrespons en beveiliging van de toeleveringsketen.

NIS2-wet (wet van 26 april 2024 Wet tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid) Versterkt de verplichtingen op het gebied van cyberbeveiliging en risicobeheer voor essentiële en belangrijke entiteiten, waaronder organisaties in de publieke sector. De richtlijn verplicht organisaties tot het implementeren van passende technische en organisatorische maatregelen op het gebied van risicoanalyse, incidentafhandeling, bedrijfscontinuïteit, beveiliging van de toeleveringsketen en kwetsbaarheidsbeheer. In de context van GenAI impliceert dit strikt toezicht op externe AI-aanbieders, verplichte incidentmelding (inclusief AI-gerelateerde beveiligingsincidenten) en versterkte verantwoordingsplicht op managementniveau voor naleving van cyberbeveiligingsvoorschriften.

Governance en rollen

Rollen & Verantwoordelijkheden

Om een formeel kader te bieden voor AI-initiatieven en -praktijken, heeft Smals de volgende bestuursorganen en rollen ingesteld.

Competency Center AI/LLM: Draagt de algehele verantwoordelijkheid voor het GenAI-beveiligingsbeleid en is voorzitter van zowel de AI Governance Board als de AI Evaluation Board.

AI Governance Board: Stelt het beleid, de normen en de richtlijnen voor GenAI vast en houdt hier toezicht op. Daarnaast beoordeelt de raad verzoeken en vragen met betrekking tot naleving voor specifieke gebruikssituaties ("use cases").

AI Evaluation Board: Beoordeelt AI-opportuniteiten en -initiatieven binnen Smals en in projecten die Smals voor haar leden beheert.

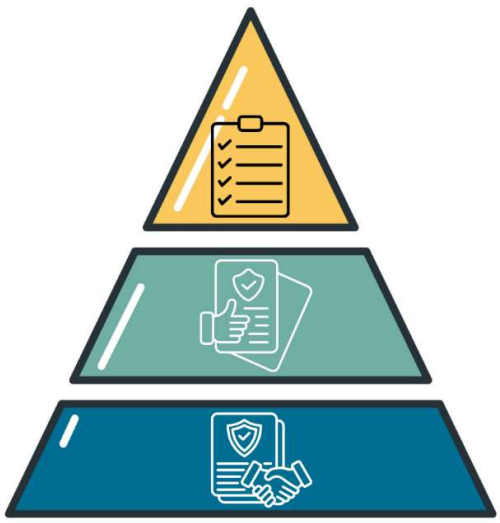
Domeineigenaar: Definieert en valideert domeinspecifieke richtlijnen en zorgt ervoor dat deze duidelijk aan eindgebruikers worden gecommuniceerd en door hen worden begrepen.

Alle medewerkers: Zijn verantwoordelijk voor het begrijpen en toepassen van de richtlijnen die relevant zijn voor hun rol en voor het escaleren van onduidelijke use cases naar de domeineigenaar en, indien nodig, de AI Governance Board.

Richtlijnen

Smals definieert een drieledig model om initiatieven op het gebied van generatieve AI efficiënt te sturen.

Verantwoorde generatieve AI: een aanpak op drie niveaus



Gebruiksspecifieke richtlijnen: implementatie	Gedetailleerde instructies voor het gebruik van generatieve AI binnen alle afdelingen en activiteiten
Standaarden	Instrumenten en processen voor de implementatie van verantwoorde AI
Smals AI-beleid: grondslagen	Kernprincipes die ten grondslag liggen aan onze aanpak

Het **Smals AI-beleid** bevat de basisregels waaraan iedereen zich moet houden. Het beschrijft de governance en definieert de fundamentele principes die altijd van toepassing zijn.

Standaarden bevat de lijst van door Smals officieel goedgekeurd generatieve AI-oplossingen, samen met de specifieke voorwaarden voor verantwoord gebruik ervan. [Deze documenten zijn momenteel in opmaak.]

Binnen het kader van de Standaarden onderscheidt Smals drie categorieën AI-tools:

1. **Lokale tools**, waarvan alle componenten uitsluitend onder de controle van Smals of een van haar leden vallen (Categorie 1).
2. **Door Smals officieel goedgekeurde tools van derden** die vallen onder een contractuele licentie met een overeenkomst inzake gegevensbescherming voor ondernemingen (Categorie 2).
3. **Niet-goedgekeurde tools van derden**. Deze categorie omvat alle gratis AI-tools of tools die onder een persoonlijke licentie vallen. In het verlengde daarvan omvat deze categorie ook alle tools die worden gebruikt op een apparaat dat niet toebehoort aan Smals of een van haar leden, zoals een persoonlijke smartphone of computer (Categorie 3).

De Standaarden hebben betrekking op alle tools in categorieën 1 en 2. Tools in categorie 3 vallen daarom buiten de Standaarden.

Gebruiksspecifieke richtlijnen worden verstrekt voor elk werkterrein binnen Smals. Deze richtlijnen helpen gebruikers het AI-beleid, het regelgevingskader en de normen te vertalen naar hun dagelijkse activiteiten en gebruikssituaties. [Deze documenten zijn momenteel in opmaak.]

Kernprincipes van het Smals AI-beleid

Het AI-beleid van Smals is gebaseerd op drie kernprincipes: **veilig en efficiënt gebruik**, **verantwoordelijkheid** en **verantwoord gebruik**. Elk principe wordt ondersteund door een reeks regels waaraan alle medewerkers van Smals zich moeten houden.

Veilig en efficiënt gebruik

1. Opleiding – Leer de tool kennen voor je hem gebruikt

Het is belangrijk dat je als nieuwe gebruiker leert hoe je generatieve AI correct inzet. Dat betekent: weten waarvoor je het mag gebruiken, hoe je een goede prompt schrijft en hoe je de output kritisch evalueert.

💡 Tip	Heb je vragen over het gebruik? Neem contact op met Smals Academy: academy@smals.be

2. Veiligheid – Gebruik alleen goedgekeurde tools

Verbind of integreer geen AI-tools met Smals-applicaties of -systemen zonder voorafgaande goedkeuring door de AI Governance Board. Gebruik **uitsluitend** tools die door Smals zijn goedgekeurd voor professioneel gebruik en die zijn opgenomen in de Standaarden.

Tools zoals ChatGPT, GitHub Copilot en Gemini draaien op externe cloudinfrastructuur. We hebben geen zicht op wat er met jouw gegevens gebeurt zodra je deze invoert. Voor tools die niet door Smals zijn goedgekeurd en niet onder een passende licentie vallen, kan informatie die in een prompt wordt ingevoerd, worden gebruikt om het AI-model verder te trainen. In sommige gevallen kunnen zelfs geanonimiseerde gegevens nog steeds naar een individu worden herleid.

Daarom kunnen de GDPR-beginselen van transparantie, doelbinding, beveiliging en opslagbeperking niet worden gegarandeerd bij het gebruik van externe tools die niet in de Standaarden zijn opgenomen.

Om datalekken en beveiligingsincidenten te vermijden, gelden de volgende strikte regels:

- Gebruik geen bedrijfsinloggegevens, e-mailadressen of telefoonnummers om je aan te melden bij publiek beschikbare GenAI-applicaties.
- Installeer geen niet-goedgekeurde API's, plug-ins, connectoren of software gerelateerd aan GenAI-systemen.
- Gebruik of implementeer code gegenereerd door GenAI nooit rechtstreeks op bedrijfssystemen zonder menselijke review.

💡 Tip

Moet je een tool gebruiken die niet in de standaarden staat? Neem contact op met de AI Governance Board om je verzoek in te dienen: AIGovBoard@smals.be

3. Vertrouwelijkheid & privacy – Deel geen gevoelige informatie

Ondanks dat er overeenkomsten voor bedrijfsgegevensbescherming bestaan die het gebruik van ingehuurde tools van derden regelen (categorie 2 van de Standaarden), is het delen van gevoelige informatie met externe AI-tools altijd verboden.

⚠️ Wat mag je NOOIT invoeren?

- Persoonsgegevens (naam, rijksregisternummer, e-mailadres, telefoonnummer, foto's, video's, ...)
- Inloggegevens, API-sleutels, certificaten en andere toegangsgegevens...
- Vertrouwelijke informatie over Smals, haar medewerkers, haar partners en leveranciers of klanten
- Alle informatie die gevoelig of vertrouwelijk is, specifiek toebehoort aan Smals, en niet bedoeld is om publiek gedeeld te worden.

✅ Aanbeveling

Als je twijfelt of de informatie die je wil gebruiken gevoelig is, neem dan contact op met je leidinggevende of stuur een email naar AIGovBoard@smals.be. Vraag altijd eerst toestemming voordat je iets doet wat een veiligheids- of privacyprobleem kan veroorzaken.

Verantwoordelijkheid

4. Menselijk toezicht – Controleer altijd de output

Generatieve AI is geen orakel. De output is niet altijd correct en de informatiebronnen achter de antwoorden zijn vaak niet transparant. Bovendien kan het model "hallucinaties" produceren: antwoorden die overtuigend klinken maar feitelijk onjuist zijn.

Gebruik AI-tools daarom uitsluitend als vertrekpunt of hulp bij het opstellen van een tekst, nooit als eindproduct. Concreet:

- Neem nooit geautomatiseerde beslissingen op basis van AI zonder menselijke tussenkomst.
- Pas een formeel dubbelcheck-proces toe als je de tool gebruikt voor kritieke taken.

5. Transparantie – Duid AI-gegenereerde inhoud aan

Alle deelnemers aan een proces – waaronder collega's, sollicitanten, Smals-leden, leveranciers en andere derde partijen – moeten worden geïnformeerd wanneer en in welke mate AI in dat proces wordt gebruikt.

Bovendien moet inhoud die volledig of gedeeltelijk door AI is gegenereerd en niet door een mens is nagelezen, duidelijk als zodanig worden gemarkeerd. Zo blijft het voor iedereen helder wat de oorsprong van de informatie is.

6. Verantwoordelijkheid – Jij blijft verantwoordelijk

De output van een AI-tool is jouw verantwoordelijkheid, niet die van het model. Controleer de inhoud altijd op correctheid, volledigheid en consistentie voordat je die gebruikt of deelt.

Verantwoord gebruik

7. Ecologische voetafdruk – Gebruik AI bewust

Generatieve AI verbruikt substantieel veel energie. Gebruik de tool doordacht: enkel wanneer het een echte meerwaarde biedt, en niet voor taken die je even snel zelf kunt uitvoeren. Vermijd het gebruik van AI-tools voor recreatieve doeleinden.

8. Maatschappelijke impact – Denk na over de gevolgen van AI voor anderen

Het integreren van generatieve AI in je processen kan veel voordelen opleveren, maar ook aanzienlijke gevolgen hebben voor je medewerkers. Wees je altijd bewust van de algemene veranderingen die dit met zich mee kan brengen.

💡 Tip	Wanneer je overweegt AI rechtstreeks in je proces te integreren, raadpleeg dan altijd de AI Governance Board om je situatie zorgvuldig te beoordelen: AIGovBoard@smals.be

Aanvaardbaar gebruik

Elk gebruik van generatieve AI via platformen, tools of software moet in lijn zijn met het beleid van Smals en de geldende wetgeving (GDPR, AI Act).

- Gebruik generatieve AI op Smals-toestellen uitsluitend voor professionele doeleinden.
- Het is verboden om via persoonlijke toestellen of accounts bedrijfsgerelateerde taken uit te voeren met generatieve AI.
- Het gebruik van generatieve AI-tools op persoonlijke toestellen om bedrijfsbeleid of -beveiligingen te omzeilen, is strikt verboden.

Samenvatting – Onthoud dit bij elk gebruik

⚠ Wees voorzichtig met wat je deelt. Je weet nooit met zekerheid wat er met jouw gegevens gebeurt.

⁉ Wees kritisch over de output. AI kan “hallucinaties” produceren: antwoorden die plausibel klinken maar fout zijn.

🏷 Duid AI-gegenereerde inhoud aan. Markeer het duidelijk als je output niet door een mens is nagelezen.

Vragen?

Heb je vragen over een specifieke use case of weet je niet zeker of jouw gebruik in lijn is met dit beleid? Neem contact op AI Governance Board – AIGovBoard@smals.be.

Blijf op de hoogte

Volg de infosessies over generatieve AI via de eAcademy:

https://eacademy.smals.be/course/view.php?id=984

Herzieningscyclus

Deze richtlijnen zijn levende documenten. Ze worden jaarlijks herzien en bijgewerkt, of onmiddellijk na een ingrijpende wijziging in de regelgeving, een beveiligingsincident waarbij AI betrokken is, of de introductie van een nieuwe GenAI-tool of -functie. Alle updates krijgen een versienummer en worden gecommuniceerd via het standaardproces voor beleidswijzigingen.

IA générative

Politique d'utilisation

Version 3.0 – June 2026
Author: Competency Center AI / LLM
Contact: AIGovBoard@smals.be

Qu'est-ce que l'IA générative ?

L'IA générative, ou GenAi en abrégé, désigne des modèles qui créent du nouveau contenu (texte, code, image, vidéo...) à partir d'une question ou d'une description. Ces modèles sont extrêmement polyvalents : la même technologie peut rédiger un texte, résumer un document, répondre à des questions ou générer du code.

À savoir : ces modèles fonctionnent de manière probabiliste. Cela signifie qu'ils ne connaissent pas une seule réponse "correcte" fixe : une même question peut donner lieu à différentes réponses. Leurs réponses s'appuient sur des modèles issus de leurs données d'entraînement, à moins que vous ne leur demandiez explicitement de fonder leur réponse sur un texte que vous leur fournissez.

ChatGPT, Claude et Gemini en sont des exemples bien connus, mais l'IA générative est également intégrée dans des outils que vous utilisez au quotidien, tels que Microsoft Office (Copilot) ou les moteurs de recherche.

Chez Smals, ces outils sont déjà activement utilisés – et faciliteront de plus en plus notre travail. Ils ne sont toutefois pas sans risque : confidentialité, exactitude, biais et confiance excessive. Cette politique vous donne des directives concrètes pour limiter ces risques.

L'accent est mis sur les outils de génération de texte et de code, car ils sont les plus répandus au sein de Smals. La présente politique évoluera au fur et à mesure que la technologie et son utilisation changeront.

Champ d'application

La présente politique s'applique à l'utilisation interne des outils d'IA générative chez Smals. Elle ne concerne pas le développement d'applications intégrant l'IA générative ; pour cela, des accords spécifiques aux projets s'appliquent.

Cadre réglementaire

Quatre cadres réglementaires européens et belges majeurs constituent le fondement de cette politique :

L'AI Act de l'Union européenne (Règlement 2024/1689) : il établit une classification des systèmes d'IA fondée sur les risques. Tout système d'IA utilisé dans le cadre de l'administration publique, de l'application de la loi ou des infrastructures critiques peut être classé dans la catégorie "à haut risque", ce qui pose des exigences en matière de supervision humaine, de transparence, de journalisation et d'évaluation de conformité.

Règlement général sur la protection des données (RGPD) / General Data Protection Regulation (GDPR) : régit le traitement des données à caractère personnel. Lorsque les outils d'IA générative traitent, génèrent ou déduisent des données à caractère personnel, les obligations du RGPD s'appliquent pleinement, y compris la base juridique, la transparence, la minimisation des données, la limitation des finalités et les droits de la personne concernée, tels que le droit à une explication des décisions automatisées. Les violations liées à l'IA et concernant des données à caractère personnel doivent être consignées et, le cas échéant, signalées dans un délai de 72 heures à l'Autorité belge de protection des données (GBA/APD), ainsi qu'aux personnes concernées en cas de risque élevé.

CyFun (Cyber Fundamentals Framework – CCB Belgique) : propose un ensemble de mesures de cybersécurité structurées autour de cinq fonctions : Identifier, Protéger, Détecter, Réagir et Restaurer. Les outils d'IA générative doivent être évalués à l'aide de ce cadre, notamment en ce qui concerne le contrôle d'accès, la traçabilité, la réponse aux incidents et la sécurité de la chaîne d'approvisionnement.

Loi NIS2 (loi du 26 avril 2024 portant établissement d'un cadre pour la cybersécurité des systèmes de réseaux et d'information d'intérêt général pour la sécurité publique) Renforce les obligations en matière de cybersécurité et de gestion des risques pour les entités essentielles et importantes, y compris les organisations du secteur public. La directive oblige les organisations à mettre en œuvre des mesures techniques et organisationnelles appropriées en matière d'analyse des risques, de gestion des incidents, de continuité des activités, de sécurité de la chaîne d'approvisionnement et de gestion des vulnérabilités. Dans le contexte de l'IA générative, cela implique une surveillance stricte des fournisseurs externes d'IA, la notification obligatoire des incidents (y compris les incidents de sécurité liés à l'IA) et une responsabilité accrue au niveau du management en matière de conformité aux règles de cybersécurité.

Gouvernance et rôles

Rôles & Responsabilités

Afin d'accompagner les initiatives et pratiques en matière d'IA d'un cadre formel, Smals a mis en place les organes de gouvernance et rôles suivants.

Centre de compétences IA/LLM : assume la responsabilité globale de la politique de sécurité relative à l'IA générative et préside à la fois l'AI Governance Board et l'AI Evaluation Board.

AI Governance Board : définit et supervise la politique, les normes et les directives relatives à l'IA générative. En outre, l'AI Governance Board évalue les demandes et les questions relatives à la conformité pour des cas d'utilisation ("use cases") spécifiques.

AI Evaluation Board : évalue les opportunités et les initiatives en matière d'IA au sein de Smals ainsi que dans les projets que Smals gère pour ses membres.

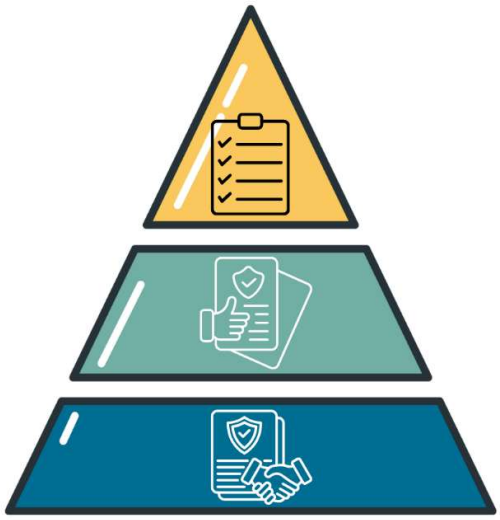
Propriétaire de domaine : définissent et valident les directives spécifiques à leur domaine et veillent à ce qu'elles soient clairement communiquées aux utilisateurs finaux et comprises par ceux-ci.

Ensemble des collaborateurs : sont tenus de comprendre et d'appliquer les directives pertinentes pour leur rôle ainsi que de remonter les cas d'utilisation ambigus au propriétaire du domaine et, si nécessaire, à l'AI Governance Board.

Directives

Smals définit un modèle en trois couches destiné à piloter efficacement les initiatives en matière d'IA générative.

IA générative responsable : une approche sur trois niveaux



Directives spécifiques à chaque usage : implémentation	Instructions détaillées relatives à l'utilisation de l'IA générative au sein de tous les services et activités
Standards	Outils et processus pour la mise en œuvre d'une IA responsable
Politique IA de Smals : principes fondamentaux	Principes fondamentaux sur lesquels repose notre approche

La **politique IA de Smals** contient les règles de base que chacun doit respecter. Elle décrit la gouvernance et définit les principes fondamentaux qui s'appliquent en toutes circonstances.

Les **Standards** rassemblent les solutions d'IA générative officiellement approuvées par Smals ainsi que les conditions spécifiques relatives à leur utilisation responsable. [Ces documents sont en cours de rédaction.]

Dans le cadre des Standards, Smals distingue trois catégories d'outils d'IA :

1. Les **outils locaux**, dont tous les composants sont exclusivement sous le contrôle de Smals ou de l'un de ses membres (catégorie 1).
2. Les **outils tiers officiellement approuvés par Smals**, qui relèvent d'une licence contractuelle assortie d'un accord sur la protection des données pour les entreprises (catégorie 2).
3. Les **outils tiers non approuvés**. Cette catégorie comprend tous les outils d'IA gratuits ou soumis à une licence personnelle. Par extension, elle inclut également tous les outils utilisés sur un appareil n'appartenant pas à Smals ou à l'un de ses membres, comme un smartphone ou un ordinateur personnel (catégorie 3).

Les Standards s'appliquent à tous les outils des catégories 1 et 2. Ils ne s'appliquent ainsi pas aux outils de la catégorie 3.

Les **directives spécifiques à un domaine** sont fournies pour chaque domaine d'activité au sein de Smals. Ces directives aident les utilisateurs à traduire la politique d'IA, le cadre réglementaire et les normes dans leurs activités quotidiennes et leurs cas d'usage. [Ces documents sont en cours de rédaction.]

Principes fondamentaux de la politique IA de Smals

La politique d'IA de Smals repose sur trois principes fondamentaux : **utilisation sûre et efficace**, **responsabilité** et **utilisation responsable**. Chaque principe s'accompagne d'une série de règles que tous les collaborateurs de Smals doivent respecter.

Utilisation sûre et efficace

1. Formation - Apprenez à connaître l'outil avant de l'utiliser

En tant que nouvel utilisateur, il est important que vous appreniez à utiliser correctement l'IA générative. Cela signifie : savoir à quelles fins vous pouvez l'utiliser, comment rédiger un prompt correctement et comment évaluer de manière critique le résultat obtenu.

💡 Conseil	Vous avez des questions sur l'utilisation ? Écrivez à Smals Academy : academy@smals.be

2. Sécurité - N'utilisez que des outils approuvés

Ne connectez ni n'intégrez aucun outil d'IA aux applications ou systèmes de Smals sans autorisation préalable de l'AI Governance Board. Utilisez exclusivement les outils approuvés par Smals pour un usage professionnel et répertoriés dans les Standards.

Les outils tels que ChatGPT, GitHub Copilot et Gemini fonctionnent sur une infrastructure cloud externe. Nous n'avons aucun contrôle sur ce qu'il advient de vos données une fois que vous les avez saisies. Pour les outils qui ne sont pas approuvés par Smals et qui ne sont pas couverts par une licence appropriée, les informations saisies dans un prompt peuvent être utilisées pour entraîner le modèle d'IA. Dans certains cas, même des données anonymisées peuvent encore être associées à un individu.

C'est pourquoi les principes du RGPD relatifs à la transparence, à la limitation des finalités, à la sécurité et à la limitation de la conservation ne peuvent être garantis lorsque des outils externes non répertoriés dans les Standards sont utilisés.

Afin d'éviter les fuites de données et les incidents de sécurité, les règles strictes suivantes s'appliquent :

- N'utilisez pas les identifiants, adresses e-mail ou numéros de téléphone de l'entreprise pour vous connecter à des applications d'IA générative accessibles au public.

- N'installez pas d'API, de plug-ins, de connecteurs ou de logiciels non approuvés liés aux systèmes d'IA générative.
- N'utilisez ou n'implémentez jamais de code généré par l'IA générative directement sur les systèmes de l'entreprise sans vérification humaine.

💡 Conseil	Vous devez utiliser un outil non répertorié dans les Standards ? Écrivez à l'AI Governance Board pour introduire votre demande : AIGovBoard@smals.be

3. Confidentialité & protection de la vie privée - Ne partagez pas d'informations sensibles

Bien qu'il existe des accords relatifs à la protection des données d'entreprise qui régissent l'utilisation d'outils tiers contractés (catégorie 2 des Standards), le partage d'informations sensibles avec des outils d'IA externes est toujours interdit.

⚠️ Quelles données ne pouvez-vous JAMAIS introduire ?

- Données à caractère personnel (nom, numéro de registre national, adresse e-mail, numéro de téléphone, photos, vidéos, etc.)
- Identifiants de connexion, clés API, certificats et autres données d'accès...
- Informations confidentielles à propos de Smals, ses collaborateurs, ses partenaires, ses fournisseurs ou ses clients.
- Toutes les informations sensibles ou confidentielles qui appartiennent spécifiquement à Smals et qui ne sont pas destinées à être rendues publiques.

✅ Recommandation

Si vous avez des doutes quant au caractère sensible des informations que vous souhaitez utiliser, adressez-vous à votre dirigeant ou envoyez un e-mail à AIGovBoard@smals.be. Demandez toujours l'autorisation avant d'entreprendre toute action susceptible de poser un problème de sécurité ou de confidentialité.

Responsabilité

4. Supervision humaine - Vérifiez toujours le résultat

L'IA générative n'est pas un oracle. Le résultat n'est pas toujours correct et les sources d'information à l'origine des réponses ne sont souvent pas transparentes. De plus, le modèle peut produire des "hallucinations", c'est-à-dire des réponses qui semblent convaincantes mais qui sont en réalité erronées.

Utilisez donc les outils d'IA uniquement comme point de départ ou comme aide à la rédaction d'un texte, jamais comme produit fini. Concrètement :

- Ne prenez jamais de décisions automatisées basées sur l'IA sans intervention humaine.
- Mettez en place un processus formel de double contrôle si vous utilisez l'outil pour des tâches critiques.

5. Transparence - Indiquez le contenu généré par l'IA

Tous les participants à un processus – y compris les collègues, les candidats, les membres de Smals, les fournisseurs et autres tiers – doivent être informés du moment et de la mesure dans lesquels l'IA est utilisée dans ce processus.

De plus, le contenu généré en tout ou en partie par l'IA et qui n'a pas été relu par un humain doit être clairement indiqué comme tel. Ainsi, l'origine de l'information reste claire pour tout le monde.

6. Responsabilité - Vous restez responsable

Le résultat produit par un outil d'IA relève de votre responsabilité et non de celle du modèle. Vérifiez toujours l'exactitude, l'exhaustivité et la cohérence du contenu avant de l'utiliser ou de le partager.

Utilisation responsable

7. Empreinte écologique - Utilisez l'IA de manière responsable

L'IA générative consomme énormément d'énergie. Utilisez cet outil à bon escient : uniquement lorsqu'il apporte une réelle valeur ajoutée, et non pour des tâches que vous pouvez accomplir vous-même rapidement. Évitez d'utiliser les outils d'IA à des fins récréatives.

8. Impact sociétal - Réfléchissez aux conséquences de l'IA pour les autres

L'intégration de l'IA générative dans vos processus peut apporter de nombreux avantages, mais aussi avoir des conséquences importantes pour vos collaborateurs. Soyez toujours conscient des changements généraux que cela peut entraîner.

💡 Conseil	Si vous envisagez d'intégrer directement l'IA dans vos processus, consultez toujours l'AI Governance Board afin d'évaluer votre situation avec soin : AIGovBoard@smals.be

Utilisation acceptable

Toute utilisation de l'IA générative via des plateformes, des outils ou des logiciels doit être conforme à la politique de Smals et à la législation en vigueur (RGPD, AI Act).

- L'utilisation de l'IA générative sur les appareils de Smals est réservée exclusivement à des fins professionnelles.

- Il est interdit d'effectuer des tâches liées à l'entreprise à l'aide de l'IA générative via des appareils ou des comptes personnels.
- L'utilisation d'outils d'IA générative sur des appareils personnels dans le but de contourner la politique ou les dispositifs de sécurité de l'entreprise est strictement interdite.

Résumé - Gardez cela à l'esprit à chaque utilisation

⚠ Faites attention à ce que vous partagez. On ne sait jamais avec certitude ce qu'il advient de vos données.

⁉ Faites preuve d'esprit critique vis-à-vis des résultats. L'IA peut produire des "hallucinations" : des réponses qui semblent plausibles mais qui sont erronées.

🏷 Indiquez clairement que le contenu a été généré par l'IA. Signalez clairement que votre contenu n'a pas été relu par un humain.

Des questions ?

Vous avez des questions concernant un cas d'utilisation spécifique ou vous ne savez pas si votre utilisation est conforme à cette politique ? Prenez contact avec l'AI Governance Board – AIGovBoard@smals.be.

Tenez-vous informé

Suivez les séances d'info consacrées à l'IA générative via eAcademy :

https://eacademy.smals.be/course/view.php?id=984

Cycle de révision

Les présentes directives sont des documents évolutifs. Elles sont révisées et mises à jour chaque année, ou immédiatement après un changement réglementaire majeur, un incident de sécurité impliquant l'IA ou l'introduction d'un nouvel outil ou d'une nouvelle fonctionnalité d'IA générative. Toutes les mises à jour reçoivent un numéro de version et sont communiquées via le processus standard de modification des politiques.