Групата ЕНЕРГО-ПРО

Политика за използването на изкуствен интелект

2025

ENERGO-PRO

Превод от английски език

Политика за използването на изкуствен интелект
Версия: 1.0 | В сила от: 01 октомври 2025 г. | Собственик: Комитет по управление на AI (AIGC)

1. Цел и обхват

1.1. Настоящата Политика за използването на изкуствен интелект („**Политиката**“) установява задължителните правила за сигурна, ефективна и отговорна употреба на инструменти с изкуствен интелект („**AI**“) в рамките на ЕНЕРГО-ПРО а.с. („**Дружеството**“) и неговите свързани лица (заедно наричани „**Групата**“). За целите на настоящата Политика, Групата означава ДК Холдинг Инвестмънтс с.р.о., едноличен акционер в Дружеството, и всички негови преки и косвени дъщерни дружества.

1.2. Нашата цел е да подкрепяме иновациите и продуктивността чрез внедряване на съвременни технологии, като същевременно гарантираме най-високо ниво на защита на нашите данни, интелектуална собственост, клиенти и репутация. Прилагането на AI трябва да се ръководи не само от стремеж към иновации, но и от твърд ангажимент към оперативната сигурност, обществената безопасност и доверието, което обществото ни гласува.

1.3. Ние сме ангажирани с това цялото използване на AI да бъде в съответствие с нашите основни етични принципи: почтеност, уважение, прозрачност и етично поведение. Човешкият надзор и отговорност остават от първостепенно значение във всички процеси, базирани на AI.

1.4. Тази Политика се прилага спрямо всички служители, външни изпълнители, консултанти и доставчици, които имат достъп до информационните системи на Групата или обработват данни на Групата (общо наричани „**Персонал**“). Политиката се отнася до всички AI Системи, използвани в рамките на Групата, независимо дали са разработени на вътрешно ниво, придобити от трети страни или достъпни като публична услуга.

2. Определения

За целите на настоящата Политика се прилагат следните определения:

2.1. AI система: AI система, както е определена в член 3, параграф 1 от Акта за AI (както е определен по-долу). Всяка система, основана на машина, предназначена да функционира с различна степен на автономност и която може да проявява адаптивност след внедряване, и която с изрични или неизрични цели, въз основа на получени входящи данни, извежда изходни данни като прогнози, съдържание, препоръки или решения, способни да влияят върху физическата или виртуална среда. Това определение се прилага независимо дали AI системата е самостоятелно приложение или е интегрирана функция в по-голям софтуерен пакет.

Корпоративен AI: Одобрена AI система, управлявана въз основа на договор (включително Допълнително споразумение за обработка на данни, както е определено по-долу), което гарантира защитата на нашите данни. Такива договори трябва изрично да забраняват на доставчика да използва данните на Групата за обучение на свои собствени модели или такива на трети страни.

Примери: Microsoft Copilot за M365, DeepL Pro.

Публичен AI: Одобрена AI система, обикновено достъпна в публичното интернет пространство, която не предоставя договорни гаранции за защита на данните и може да използва входовете (заявките) и изходите (отговорите) за обучение или подобряване на своите модели или такива на трети страни.

Примери: Стандартни версии на ChatGPT, Google Gemini, Google Translate.

2.2. **Класификация на данните**: Всички данни се класифицират в четири нива:

Публични (Ниво 1): Всяка информация, която по закон е в публичното пространство. Това включва както информация, официално публикувана от Групата, така и информация от външни публични източници.

Примери: Публикувани прессъобщения, академични публикации, новинарски статии, публични правителствени бази данни, информация на публично достъпни уебсайтове.

Вътрешни (Ниво 2): Непублична информация, неразрешеният достъп до която води до ниско ниво на риск.

Примери: Протоколи от общи екипни срещи (които не съдържат лични данни или търговски тайни), вътрешни ръководства, проектни чернови без чувствителен характер.

Поверителни (Ниво 3): Чувствителни данни, чието разкриване може да причини умерена до сериозна вреда на Групата, нейните партньори или клиенти.

Примери: Финансови планове, бизнес стратегии, неодитирани финансови резултати, анонимизирани договори.

Строго поверителни (Ниво 4): Най-чувствителните данни, защитени от закон или договор, чието неразрешено разкриване може да доведе до сериозни правни, финансови или репутационни вреди.

Примери: Лични данни по смисъла на ОРЗД (както е определен по-долу) (напр. данни за служители или клиенти), търговски тайни, чувствителна информация по отношение на ценообразуването, информация, защитена с договор за поверителност, ноу-хау, данни за достъп до системи и пароли, сорс код, оперативни данни от критична инфраструктура (напр. системи SCADA), подробни оценки на уязвимости на електрическата мрежа, или схеми на електроенергийни производствени съоръжения.

2.3. Допълнително споразумение за обработка на данни (ДСОД): Правно обвързващ договор, сключен между администратор на данни и обработващ данните съгласно член 28 от ОРЗД. Той урежда обработката на лични данни от страна на обработващия от името на администратора. Такова споразумение е задължително по ОРЗД, когато администраторът възлага обработка на обработващия лични данни.

2.4. Дийпфейк: Всяко AI-генерирано или AI-манипулирано видео, аудио или изображение, което наподобява реални лица, обекти, места, теми или събития и на обикновен наблюдател може да изглежда като автентично или достоверно.

2.5. Халюцинация: Явление, при което модел с изкуствен интелект генерира отговори, които са безсмислени, фактически неверни или напълно измислени, въпреки че ги представя с увереност и убедителност.

2.6. Запитване: Всеки вход – като въпрос, инструкция или набор от данни – предоставен от потребител към AI система с цел получаване на изход (отговор).

3. Роли, отговорности и управление

Комитет по управление на AI (AIGC): Интердисциплинарен екип, съставен от представители на висшето ръководство, Правен отдел, Човешки ресурси и други ключови отдели. Комитетът одобрява стратегията за AI, настоящата Политика и носи отговорност за поддържането на Регистъра.

AI Навигатор: Основно лице за контакт за насоки и подкрепа по въпроси, свързани с AI. Тази роля предоставя проактивни съвети, подпомага AIGC и съдейства на Персонала при въпроси, свързани с AI.

Собственик на AI система: Освен ако Комитетът по управление на AI (AIGC) не реши друго, AI Навигаторът изпълнява ролята на Собственик на AI системата за всяка одобрена AI система. Собственикът на AI системата носи отговорност:

1. да гарантира, че AI системата се използва единствено за одобрената ѝ цел и в рамките на разрешените ѝ параметри;

2. да служи като основно лице за контакт при одити и прегледи на ефективността;

3. да управлява достъпа на потребители в координация с ИТ отдела; и

4. да докладва всички съществени проблеми с производителността или инциденти на AI Навигатора с цел ескалация към AIGC.

Персонал: Всеки член на Персонала е длъжен да разбира и спазва настоящата Политика.

4. Основни принципи за използване на AI

Всяко използване на AI в рамките на Групата трябва да бъде в съответствие със следните ключови принципи:

4.1. Човек, участващ в процеса (Задължителен надзор от човек): AI е помощен инструмент и не взема автономни решения. AI системата може да подпомага и разширява човешките способности, но не заменя човешката преценка и отговорност. Всички отговори, генерирани от AI – особено такива с потенциални правни или финансови последици – трябва да бъдат критично прегледани, проверени и одобрени от квалифицирано и отговорно лице преди използването им. Степента на преглед следва да е пропорционална на риска от

вземаното решение (напр. проверката на единичен факт в доклад изисква по-малко внимание от одобряването на график за поддръжка на мрежа, генериран от AI).

4.2. Отговорност: Крайната отговорност за всяко решение или действие, основано на резултат, генериран от AI, носи лицето, което го използва, а не самата AI система. Персоналът трябва да бъде бдителен във връзка с възможността AI да генерира „халюцинации“ и винаги трябва да проверява критичната информация чрез независим и надежден източник.

4.3. Прозрачност: Когато AI система е проектирана да взаимодейства директно с физически лица (например чрез чатбот), тези лица трябва да бъдат информирани, че взаимодействат със AI система. Персоналът, който генерира или манипулира изображение, аудио или видео съдържание, което изглежда автентично (включително илюстрации за маркетингови материали, създадени с AI, както и дийпфейкове), трябва ясно и видимо да посочи, че съдържанието е генерирано или променено посредством изкуствен интелект – както е допълнително посочено в раздел 6.3(iii).

4.4. Недопускане на дискриминация и справедливост: Системите с AI трябва да се използват по начин, който избягва създаването или затвърждаването на несправедливи предразсъдъци или дискриминация спрямо лица или групи въз основа на защитени признаци (напр. възраст, пол, етническа принадлежност).

4.5. Сигурност и защита на личните данни по замисъл: Защитата на данните и сигурността са от основно значение. Всички проекти, свързани с AI – от етапа на придобиване до внедряване и евентуално извеждане от експлоатация – трябва да интегрират принципите за поверителност и сигурност още от самото начало.

5. Приложимо законодателство и вътрешни политики

5.1. Правна и регулаторна рамка

5.2. Разработването, придобиването и използването на AI Системи от страна на Групата се уреждат от рамка от приложими закони и международни стандарти. Всички членове на Персонала са длъжни да спазват най-новите версии на следните разпоредби, включително, но не само:

Регламент (ЕС) 2024/1689 на Европейския парламент и на Съвета от 13 юни 2024 г. относно установяване на хармонизирани правила за изкуствения интелект („**Акт за AI“**).

Регламент (ЕС) 2023/2854 на Европейския парламент и на Съвета от 13 декември 2023 г. относно хармонизирани правила за справедлив достъп до данни и използването им (**„Акт за данните“).**

Директива (ЕС) 2022/2555 на Европейския парламент и на Съвета от 14 декември 2022 г. относно мерки за високо общо ниво на киберсигурност в рамките на Съюза („**Директива NIS 2“**).

Директива (ЕС) 2019/790 на Европейския парламент и на Съвета от 17 април 2019 г. относно авторското право и сродните му права в цифровия единен пазар („**Директива за авторското право**“).

Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 г. относно защитата на физическите лица при обработването на лични данни и относно свободното движение на такива данни („**ОРЗД**“).

ISO/IEC 42001:2023 – Информационни технологии — Изкуствен интелект — Система за управление.

Цялото приложимо национално законодателство в юрисдикциите, в които Групата осъществява дейност, включително, но не само, нормативни актове, уреждащи трудовото право, правото на интелектуална собственост и гражданската отговорност.

5.3. Връзка с други вътрешни политики

5.4. Настоящата Политика допълва и следва да се тълкува съвместно с други задължителни политики на Групата. Персоналът следва също така да гарантира, че използването на AI Системи е в съответствие с всички други приложими вътрешни политики, включително, но не само:

- Кодекс за поведение
- Политика за правата на човека
- Политика по управление на човешките ресурси
- Политика по сигурността
- Политики за защита на данните (вътрешни и външни)
- План за управление на изпълнителите и подизпълнителите

5.5. В случай на противоречие между настоящата Политика и друга вътрешна политика, се прилага по-ограничаващото разпореждане. Въпросът следва незабавно да се отнесе до AI Навигатора за разяснение от страна на AIGC.

6. Допустима и забранена употреба

6.1. Златното правило: Съответствие между данните и подходящата AI система.

Най-важният принцип е да се гарантира, че данните се обработват единствено от AI система, която осигурява съответстващо ниво на сигурност. Неспазването на този принцип представлява сериозно нарушение на настоящата Политика.

Класификация на данни	**Публичен AI**	**Корпоративен AI**
Ниво 1: Публични	Разрешено	Разрешено
Ниво 2: Вътрешни	Разрешено	Разрешено
Ниво 3: Поверителни	Разрешено с ограничения	Разрешено
Ниво 4: Строго поверителни	Забранено	Разрешено само с одобрение от AIGC и при задължително провеждане на DPIA (оценка на въздействието върху защитата на данните) и оценка на риска за ИТ сигурността.

6.2. Одобрени AI Системи

Общо правило

На Персонала е разрешено да използва само онези AI Системи, които са включени в официалния „Регистър на одобрените AI Системи“ („**Регистъра**“). Използването на каквато и да е AI система, която не е включена в Регистъра, е строго забранено. Списък на Системите с AI, одобрени към датата на влизане в сила на настоящата Политика, е приложен за справка като Приложение А. Водещата и актуализирана версия на Регистъра се поддържа и редовно актуализира от AIGC и е достъпна в M365 SharePoint на Групата.

Използване на AI Системи с минимален риск

Независимо от горепосоченото правило, на Персонала е разрешено да използва AI система, която не е включена в Регистъра, при условие че такава система отговаря на определението за „AI система с минимален риск“ съгласно класификацията в Раздел 8 от настоящата Политика. Лицето, което възнамерява да използва системата, носи пълната отговорност за нейното правилно оценяване и класифициране като AI система с минимален риск.

Лице, което се възползва от това изключение, следва без ненужно забавяне да уведоми AI Навигатора за използването на такава AI система по имейл. Използването на такава система трябва във всеки един момент да бъде в пълно съответствие с настоящата Политика и всички останали политики на Групата, включително, но не само, тези относно защита на данните (ОРЗД), информационна сигурност и ИТ сигурност.

Използване на Публични AI Системи за данни от Ниво 3 (Поверителни)

Обработката на данни от Ниво 3 (Поверителни) чрез Публични AI Системи е строго забранена, освен ако са изпълнени всички долупосочени условия:

(i) Използваната Публична AI система трябва да е одобрена за тази цел в Регистъра и да се използва в съответствие с посочените в него условия. Към датата на последната ревизия на настоящата Политика, изискваните методи са:

• **За Adobe Acrobat AI Assistant:** Одобрен за използване без необходимост от допълнителни настройки за защита на личните данни. Архитектурата му, изградена на принципа „защита на личните данни по замисъл“, гарантира, че потребителските данни са изолирани и не се използват за обучение на модели.

• **За ChatGPT:** Задължително трябва да се използва функцията „Временен чат“ (Temporary Chat).

• **За Google Gemini:** Настройката „Gemini Apps Activity“ трябва да бъде изключена.

• **За NotebookLM:** Одобрен за използване без необходимост от допълнителни настройки за защита на личните данни. Архитектурата му по замисъл гарантира, че потребителските данни са изолирани и не се използват за обучение на модели.

(ii) Условията за ползване на Публичната AI система трябва да гарантират, че потребителските запитвания (prompts) и отговори (изходи) няма да бъдат използвани за обучение или подобряване на модели на доставчика или на трети страни.

(iii) Запитванията и отговорите от сесията не трябва да се запазват в постоянната история на разговорите на потребителя и трябва да подлежат на автоматично изтриване от страна на доставчика. Потребителите трябва да потвърдят, че са запознати с периода на съхранение за цели, свързани със сигурността и поддръжката, който към момента е:

- До 30 дни за ChatGPT „Temporary Chat“;
- До 72 часа (3 дни) за Google Gemini с изключена „Activity“.

Отговорност на потребителя е да избере правилната функция и да се запознае с приложимия срок за съхранение на данни преди да въведе данни от Ниво 3 (Поверителни) в Публична AI система.

6.3. Забранени дейности

Използването на AI за следните цели е строго забранено:

(i) Всякаква дейност, която противоречи на приложимото законодателство, по-специално забранените практики, определени в член 5 от Акта за AI, или нарушава Кодекса за поведение на Групата или която и да е друга приложима вътрешна политика.

(ii) Въвеждане на данни от Ниво 4 в каквато и да е Публична AI система или въвеждане на данни от Ниво 3 в Публична AI система без спазване на ограниченията, посочени в Раздел 6.2.

(iii) Забранено е създаването или разпространението на дийпфейкове и други синтетични медии, генерирани от AI, с вредоносна, измамна или подвеждаща цел – или по какъвто и да е начин, който има за цел или има висока вероятност може да заблуди дадено лице, че съдържанието е автентично.

Създаването и използването на изображения, аудио, видео или сходни резултати, генерирани или манипулирани чрез AI, в други случаи е разрешено за легитимни илюстративни, образователни, дизайнерски, обучителни или други бизнес цели, при спазване на следните условия:

а. съдържанието е ясно обозначено пред аудиторията като генерирано/манипулирано с AI (например чрез надпис върху съдържанието, пояснение, воден знак, метаданни, бележка под линия на слайд или друга съпътстваща информация, видима в момента на използване); и
б. съдържанието не се представя като фактически запис на реални лица, обекти, места, теми или събития.

(iv) Създаване и използване на реалистични, подобни на хора аватари с цел имитиране или подвеждащо взаимодействие със служители, клиенти или обществото.

(v) Вземане на окончателни, автоматизирани решения относно физически лица (напр. при подбор на персонал, оценки на представянето или прекратяване на трудов договор) без реален човешки надзор и преглед.

(vi) Всеки опит за заобикаляне на мерките за сигурност или ограниченията за използване на одобрена AI система.

6.4. Препоръчителни дейности

Ние приветстваме и насърчаваме използването на одобрени AI Системи. Следният списък е илюстративен, но не изчерпателен, и представя примери за полезни приложения:

(i) Подпомагане при създаване на имейли, доклади или презентации.

(ii) Превод на документи (в съответствие с правилата за класификация на данните).

(iii) Обобщаване на документи и анализиране на данни с цел откриване на нови изводи.

(iv) Генериране на идеи и създаване на концептуални проекти.

(v) Автоматизиране на повтарящи се задачи (напр. създаване на формули в електронни таблици).

(vi) Първоначално изготвяне на технически доклади относно тенденции на енергийния пазар на база публични данни, като всички факти и числа след това се проверяват от експерт в съответната област.

При всяко потенциално приложение, което не е изрично посочено по-горе, Персоналът трябва да действа с повишено внимание и да гарантира, че предлаганата употреба е в пълно съответствие с основните принципи на настоящата Политика, както и с всички други приложими нормативни и вътрешни правила. Винаги трябва да се извършва професионална преценка. При каквото и да е съмнение относно допустимостта или съответствието на предложената употреба, консултация с AI Навигатора е задължителна преди предприемане на действия.

7. Придобиване и одобрение на AI Системи

7.1. Всяка нова AI система трябва да премине през следния процес на одобрение, преди да може да бъде използвана:

(i) Подаване на заявление: Лице подава искане чрез официален формуляр (вж. Приложение Б).

(ii) Първоначална оценка: AI Навигаторът преглежда искането спрямо основните критерии.

(iii) Оценка на риска: AIGC извършва подробна оценка на риска (вж. Раздел 8).

(iv) Решение: AIGC одобрява, отхвърля или одобрява с определени ограничения AI системата.

(v) Регистрация: Одобрената AI система се вписва в Регистъра.

8. Оценка на риска и класификация на системите

8.1. Всяка AI система се класифицира съгласно четиристепенния модел на риск, определен в Акта за AI:

Недопустим риск: AI Системи, които са забранени от закона и от настоящата Политика (напр. социално оценяване – "social scoring").

Висок риск: AI система, която отговаря на критериите, изложени в член 6 от Акта за AI, включително, но не само, системи, които могат съществено да повлияят върху здравето, безопасността или основните права на лицата (напр. AI система, използвана за управление на критична инфраструктура или за филтриране на кандидатури за работа). Такива системи подлежат на по-строги изисквания, включително задължителна регистрация, строги тестове и непрекъснат мониторинг.

Среден риск: Тази категория обхваща AI Системи, които създават специфични рискове, свързани с манипулация или заблуда, поради което подлежат на конкретни изисквания за прозрачност. Тези изисквания варират в зависимост от типа AI система и конкретното ѝ приложение:

- **Системи за директно взаимодействие (напр. чатботове):** При използване на системи, предназначени за директно взаимодействие с лица – като чатботове за

вътрешна поддръжка по ЧР или външно обслужване на клиенти – потребителите трябва ясно да бъдат информирани, че комуникират със AI система.

- **Синтетични медии (изображения, аудио, видео):** Системите с AI, използвани за генериране или манипулиране на реалистични изображения, аудио или видео съдържание (напр. дийпфейкове), трябва ясно да обозначават отговора си като „генериран от AI“ или „изкуствено манипулиран“, освен ако съдържанието очевидно има художествен или креативен характер и не цели представяне на реалност.

- **Системи с общо предназначение (GPAI) за генериране на текст:** Основните модели на инструменти като ChatGPT, Gemini и Copilot се считат за Системи с общо предназначение (GPAI) и се подчиняват на изисквания за прозрачност от страна на техните доставчици. За нашите цели, когато тези инструменти се използват като помощни средства – напр. за обобщаване на текст, съставяне на имейли или генериране на идеи – генерираният текст не подлежи на задължително обозначаване като създаден от AI, при условие че е подложен на реален преглед от човек и редакционен контрол преди използване. В тези случаи AI действа като асистент, а пълната отговорност за съдържанието носи Персоналът.

Минимален риск: Тази категория се отнася до AI Системи, които представляват пренебрежим риск за правата, свободите или сигурността на физически лица. Система се класифицира като AI система с минимален риск само ако отговаря на всички долупосочени условия:

- Не взема решения или не прави преценки, които засягат правата на физически лица;
- Не обработва чувствителни лични данни; и
- Потенциална повреда или грешен резултат не биха довели до съществено отражение върху сигурността.

AI система може да бъде прекласифицирана в по-висока рискова категория (Среден или Висок риск), ако целта на използване бъде променена така, че да включва обработка на лични, биометрични или критични за сигурността данни. Макар Системите с минимален риск да не се регулират изрично от Акта за AI, тяхното използване трябва да бъде в съответствие с общите принципи, изложени в настоящата Политика.

Примери за AI Системи с минимален риск: Спам филтри, базирани на AI, Модели за прогнозиране на времето, Системи за управление на складови наличности с AI за прогнозиране на търсенето, Помощни средства за граматическа и правописна проверка в текстообработващи програми и имейл клиенти, Инструменти за машинен превод (напр.

автоматичен превод на уебсайтове), използвани само за бързо разбиране (преводът на публично достъпен текст създава незначителен риск само ако не съдържа чувствителни данни)

9. Защита на данни, интелектуална собственост и сигурност

Защита на личните данни по замисъл (Privacy by Design): Принципът за защита на личните данни по замисъл и по подразбиране трябва да бъде интегриран във всеки проект, свързан с AI, още от самото начало.

Оценка на въздействието върху защитата на данните (DPIA): Оценката на въздействието върху защитата на данните (виж Приложение B) е задължителна за всяка AI система, която вероятно ще доведе до висок риск за правата и свободите на физическите лица.

Интелектуална собственост върху съдържание, генерирано от AI: Персоналът трябва да е наясно, че правният статут на съдържанието, генерирано от AI, е сложен и подлежи на развитие. Освен ако не е изрично посочено друго в условията за използване на одобрена AI система, резултатите, генерирани от AI, може да не подлежат на закрила чрез авторско право или да са обект на права на трети страни. Цялото съдържание, създадено чрез AI в хода на трудовото правоотношение, се счита за служебен резултат на Групата, но персоналът не бива да приема, че Групата притежава изключителни авторски права върху него. Използването на съдържание, генерирано от AI, в материали с публична насоченост или в търговски продукти изисква предварителна консултация с AI навигатора.

Защита на поверителна информация и интелектуална собственост: Персоналът трябва да проявява изключителна предпазливост за защита на чувствителната информация на Групата. Това включва, но не се ограничава до, търговски тайни, чувствителна ценова информация, ноу-хау, информация, защитена с договори за поверителност, авторски права и права на индустриална собственост. Както е посочено в Раздел 6, такава информация никога не бива да се въвежда в публична AI система.

Сигурност: Всички AI системи трябва да отговарят на установените ни стандарти за киберсигурност.

10. Мониторинг, докладване и метрики

Ще осъществяваме мониторинг на представянето, точността и сигурността на нашите AI системи.

За AI системи с висок риск са задължителни редовни доклади до AIGC. Ще измерваме не само техническите параметри, но и генерираната бизнес стойност (напр. спестено време, подобрения в процесите).

11. Реакция при инциденти и управление на промени

Инциденти: Всеки инцидент, свързан с AI система (напр. пробив на данни, грешен резултат със значително въздействие, подозрения за дискриминация), трябва незабавно да се докладва на AI навигатора.

Промени: Всяка съществена промяна в AI система (напр. нова версия, промяна в предназначението) изисква нова оценка на риска от AIGC. Съществена промяна включва, но не се ограничава до следните: промяна в предназначението на системата, внедряване на нова основна версия на модела или значителна промяна в данните за вход/изход.

12. Обучение на персонала и AI грамотност

Задължително обучение: Всички служители трябва редовно да преминават задължително обучение относно използването на AI. Това обучение ще се провежда поне веднъж годишно и ще обхваща настоящата политика, сигурност на данните, осведоменост относно рискове (вкл. дискриминация и халюцинации) и правилна употреба на одобрени AI системи.

Надграждащо обучение: Предоставя се на служители, които работят интензивно с AI, с фокус върху сигурността на данните, осведомеността за рисковете (включително дискриминация) и правилното използване на одобрени системи с изкуствен интелект. Допълнително обучение ще се провежда при необходимост, например след значителни актуализации на законовите разпоредби или нашите системи с изкуствен интелект.

AI портал: Вътрешен SharePoint сайт, който служи като централен ресурсен хъб за всички въпроси, свързани с AI. Съдържа регистъра, ръководства за потребителя, учебни материали, политики и данни за контакт.

13. Управление на трети страни и доставчици

Преди придобиването на каквато и да е корпоративна AI система доставчикът подлежи на процес на надлежна проверка (дю дилиджънс). Тази оценка следва да разгледа нивото на

сигурност на доставчика, наличните му сертификати за съответствие, репутацията му и степента на прозрачност по отношение на AI моделите, които използва.

Задължително условие (неподлежащо на преговори): Необходимо е да имаме подписано Допълнително споразумение за обработка на данни (ДСОД) с всеки доставчик, чиято AI система ще обработва наши непублични данни (нива 2–4). Това ДСОД трябва изрично да забранява на доставчика да използва нашите данни за обучение на своите модели.

14. Преглед и одит на политиката

Настоящата политика е „жив документ“. AIGC (Комитетът по управление на AI) ще я преглежда и актуализира най-малко веднъж годишно или по-често – в отговор на значими технологични или законодателни промени. Вътрешният одит периодично ще проверява спазването на тази политика.

15. Санкции при неспазване

Нарушаването на настоящата политика се счита за сериозно нарушение на служебните задължения и може да доведе до дисциплинарни мерки съгласно вътрешните правила и приложимото законодателство, включително и до прекратяване на трудовото или договорното правоотношение.

16. Приложения (налични в AI портала)

- **Приложение А:** Регистър на одобрените AI системи
- **Приложение Б:** Формуляр - искане за одобрение на нова AI система
- **Приложение В**: Шаблон за оценка на въздействието върху защитата на данните (DPIA)
- **Приложение Г**: Данни за контакт

Приложение А: Регистър на одобрените AI системи

Последна актуализация: 21 юли 2025 г. | **Поддържа се от:** AI навигатора

Настоящият регистър съдържа окончателен списък на AI системите, които са били оценени и одобрени за използване в рамките на Групата. Всяка AI система, която не е включена в този списък, се счита за забранена, освен ако не е предоставено изрично одобрение от Комитета по управление на AI (AIGC).

Име на AI системата	**Категория**	**Класификация на риска**	**Примери за одобрени случаи на използване**	**Макс. разрешено ниво на класификация на данните**	**Статус**
Adobe Acrobat AI Assistant	Публична AI	Ограничен риск	AI асистентът бързо анализира документи, за да направи основни изводи, идентифицира модели и отговаря на сложни въпроси, като всички отговори са директно свързани с източниците в текста.	Ниво 3 (Поверително) – с ограничения	Одобрена
Celsia AI Assistant	Корпоративна AI	Ограничен риск	Филтриране на релевантна информация от вътрешни документи на Групата, създаване на кратки резюмета и отговаряне на въпроси, свързани с ESG.	Ниво 4 (Строго поверително)	Одобрена
ChatGPT (безплатна/ Plus версии)	Публична AI	Ограничен риск	Съставяне на имейли, обобщаване на документи, генериране на идеи, превод на текст.	Ниво 3 (Поверително) – с ограничения	Одобрена
DeepL Pro	Корпоративна AI	Ограничен риск	Превод на документи, включително съдържащи строго поверителна информация.	Ниво 4 (Строго поверително)	Одобрена
Google Gemini	Публична AI	Ограничен риск	Съставяне на имейли, обобщаване на документи, генериране на идеи, превод на текст.	Ниво 3 (Поверително) – с ограничения	Одобрена

Име на AI системата	Категория	Класификация на риска	Примери за одобрени случаи на използване	Макс. разрешено ниво на класификация на данните	Статус
Google Translate	Публична AI	Ограничен риск	Превод само на неповерителна, публична информация.	Ниво 2 (Вътрешна)	Одобрена
Microsoft Copilot for M365	Корпоративна AI	Ограничен риск	Съставяне на имейли, обобщаване на документи и срещи, анализ на данни в рамките на приложенията на Microsoft 365.	Ниво 4 (Строго поверително)	Одобрена
NotebookLM	Публична AI	Ограничен риск	Превръщане на конкретни проектни документи, изследвания и бележки от срещи в интерактивен експерт, който може да предоставя резюмета, фактически отговори и нови прозрения, базирани единствено на лични източници.	Ниво 3 (Поверително)	

Приложение Б: Формуляр - искане за одобрение на нова AI система

Моля, попълнете този формуляр изцяло и го изпратете до AI навигатора за всяка нова AI система, която желаете да използвате за нуждите на Групата.

Раздел 1: Информация за заявителя

- Пълно име:
- Отдел:
- Длъжност:
- Дата на заявката:

Раздел 2: Данни за AI системата

- Име на AI системата:
- Доставчик/платформа:
- Линк към уебсайта на системата:
- Линк към Политиката за поверителност / Общите условия:

Раздел 3: Предназначение

- **Бизнес цел**: (Моля, опишете бизнес проблема, който се стремите да разрешите, и как тази AI система ще помогне. Каква е основната цел?)

- **Конкретни задачи**: *(*Избройте конкретните задачи, които възнамерявате да извършвате с тази AI система, напр. „Превод на правни договори“, „Създаване на маркетинг съдържание“, „Анализ на обратна връзка от клиенти“.)

Раздел 4: Използване на данни

- **Кое е най-високото ниво на класификация на данните, което възнамерявате да обработвате с тази AI система?**

  (Виж Раздел 2.2 от AI Политиката)

  - o [ ] Ниво 1: Публична информация
  - o [ ] Ниво 2: Вътрешна информация
  - o [ ] Ниво 3: Поверителна информация
  - o [ ] Ниво 4: Строго поверителна информация

• Ще обработва ли AI системата лични данни, както са определени в ОРЗД?

o [ ] Да

o [ ] Не

• Ще се използва ли AI системата за вземане на решения, които имат съществено въздействие върху физически лица (напр. подбор на персонал, оценка на представяне)?

o [ ] Да

o [ ] Не

Раздел 5: Първоначална оценка на риска

• Предоставя ли доставчикът Допълнително споразумение за обработка на данни (ДСОД), което изрично забранява използването на нашите данни за обучение на негови модели или такива на трети лица?

o [ ] Да

o [ ] Не

o [ ] Не знам

• До колкото ви е известно, съществуват ли известни уязвимости по отношение на сигурността или етични притеснения, свързани с тази AI система? (Ако да – моля, посочете подробности.)

Само за вътрешна употреба от AIGC

• ID на заявката:

• Дата на получаване:

• Оценка от AI навигатора: Завършена / Незавършена

• Решение на AIGC: Одобрена / Отхвърлена / Одобрена с ограничения

• Дата на решението:

• Обосновка / Ограничения:

Приложение B: Шаблон за оценка на въздействието върху защитата на данните (DPIA) за AI система

Този шаблон трябва да бъде попълнен за всяка AI система, класифицирана като **високорискова**, или за всяка AI система, която обработва данни с **ниво 4 (Строго поверителни**), особено когато се обработват лични данни в голям мащаб или обработката вероятно ще доведе до висок риск за правата и свободите на физическите лица.

DPIA референция: [Уникален идентификатор]

Име на AI системата: [Име на AI системата]

Собственик на AI системата: [Име]

Дата на оценката: [Дата]

Част 1: Описание на обработката

• **Характер и обхват на обработката:** Опишете функционалността на AI системата, вида данни, които ще се обработват, обема на данните и категориите на субектите на данни.

• **Цел на обработката:** Какви са очакваните резултати и ползи за Групата, клиентите или служителите?

• **Контекст на обработката:** Опишете взаимоотношението със субектите на данни и техните разумни очаквания. Посочете източниците на данни и всички потоци от данни към трети страни.

Част 2: Оценка на необходимостта и пропорционалността

• **Правно основание:** Какво е правното основание за обработка на лични данни съгласно чл. 6 от ОРЗД?

• **Ограничение на целите:** Обработват ли се данните единствено за конкретни, изрично посочени и легитимни цели?

• **Минимизиране на данните:** Обработват ли се данните в обем, който е адекватен, относим и ограничен до необходимото за постигане на целите на обработката?

Част 3: Оценка на рисковете

• **Рискове за правата и свободите на субектите на данни:** Идентифицирайте потенциалните рискове, например:

o Неоторизиран достъп или пробив в сигурността на данните.

o Неточни резултати, водещи до неправилни решения.

o Дискриминационен уклон в резултатите (напр. при подбор на персонал или кредитна оценка).

o Липса на прозрачност или обяснимост при вземане на решения, базирани на AI.

o Повторна идентификация на анонимизирани или псевдонимизирани данни.

• **Вероятност и тежест на риска: За** всеки идентифициран риск оценете вероятността от настъпването му (Ниска / Средна / Висока) и потенциалната тежест на въздействието.

Част 4: Предвидени мерки за ограничаване на риска

• **Технически мерки:** Опишете приложените мерки за сигурност (напр. криптиране, контрол на достъпа, псевдонимизация).

• **Организационни мерки:** Опишете процедурните контроли (напр. човешки надзор, регулярни одити, обучение на персонала, ДСОД с доставчика).

• **Ограничаване на алгоритмичната пристрастност:** Опишете предприетите стъпки за тестване и ограничаване на пристрастността в алгоритъма.

• **Мерки за прозрачност:** Как ще бъдат информирани субектите на данни относно използването на AI системата и техните права?

Част 5: Консултации и одобрение

• **Консултация с длъжностното лице по защита на данните (ДЛЗД):** Запишете становището, предоставено от длъжностното лице по защита на данните.

Решение на Комитета по управление на AI (AIGC):

o [ ] Пристъпване към обработката.

o [ ] Пристъпване към обработката след прилагане на допълнителни мерки.

o [ ] Да не се пристъпва към обработката.

o [ ] Консултация с надзорния орган.

Одобрение:
• **Собственик на AI системата:** _____
• **Длъжностно лице по защита на данните (ДЛЗД):** _____
• **Председател на AIGC:** _____

Приложение Г: Данни за контакт

За всякакви запитвания относно настоящата политика или използването на AI в рамките на Групата, моля, свържете се със съответните лица:

Основно лице за контакт

- **AI навигатор**
  - **Име**: Томаш Брандейски (Tomáš Brandejský)
  - **Имейл**: t.brandejsky@energo-pro.com
  - **Отговорности**: Поддръжка от първо ниво за персонала, координиране на обучения и управление на процеса по одобрение на AI системи.

Управление и ескалация

- **Комитет по управление на AI (AIGC)**
  - **Председател**: Якуб Файфр (Jakub Fajfr)
  - **Главен юрисконсулт**: Кристиан Блачфорд (Christian Blatchford)
  - **Длъжностно лице по защита на данните** (ДЛЗД): Марина Радева
  - **Ръководител „Човешки ресурси**“: Никола Шугра (Nikola Šugra)
  - **Имейл**: AIGC@energo-pro.com
  - **Отговорности**: Стратегически надзор, одобрение и редовно актуализиране на Регистъра на одобрените AI системи, одобрение на политиката за AI, управление на рискове и окончателно одобрение за AI системи с висок риск.

Долуподписаната, Ася Тодорова Михайлова, удостоверявам верността на извършения от мен превод от английски на български език на приложения документ . Преводът се състои от 22 страници.

Заклет преводач:
Ася Тодорова Михайлова