

— PACK VALIDATION · SÉCURITÉ, RGPD & IA ACT

Convaincre votre DSI, votre RSSI et votre DPO.

Le dossier prêt à transmettre pour obtenir le feu vert sécurité et conformité sur Cortex × Impact³.

Architecture, hébergement, RGPD, IA Act : les réponses, les preuves et le parcours de validation, section par section, pour que la conformité avance aussi vite que le métier.

VOTRE DSI

Architecture & intégration

Chaîne technique hébergée en UE, flux de données, réversibilité : un système qui se branche, pas un chantier SI.

PAGES 04 · 05

VOTRE RSSI

Sécurité & preuves

Quatre principes, une chaîne attestée de bout en bout et des preuves vérifiables en temps réel, sans nous croire sur parole.

PAGES 06 · 07

VOTRE DPO

RGPD & IA Act

Article 28, DPA, sous-traitants ultérieurs listés et positionnement IA Act : un cadre contractuel, pas une zone grise.

PAGES 08 · 09

LA CHAÎNE,
EN UN COUP D'ŒIL

Application ·
OVHcloud

UE / FRANCE · ISO · HDS

→ Backend ·
Supabase

UE · SOC 2 TYPE II

→ Couche IA · Anthropic

→ ATTESTÉE · ZDR · SANS
ENTRAÎNEMENT

POURQUOI CE PACK, ET COMMENT L'UTILISER

Votre projet est validé métier. Reste le feu vert IT et conformité.

Les projets d'IA aux Achats échouent rarement sur la valeur métier. Ils s'enlisent dans la boucle de validation : la DSI attend un dossier d'architecture, le RSSI des preuves, le DPO un cadre RGPD, et chacun découvre le sujet séparément. Ce pack réunit les trois dossiers en un. Transmettez à chacun sa section, telle quelle, et gagnez un cycle complet de validation.

QUI REÇOIT QUOI

CHAQUE SECTION SE TRANSMET TELLE QUELLE

Votre Direction Générale	PAGE 03	L'argument du cadre : l'IA générative est déjà utilisée par vos équipes. La vraie décision ne porte pas sur son autorisation, mais sur sa gouvernance.
Votre DSI	PAGES 04 - 05	Architecture, hébergement, flux de données, intégration au SI et réversibilité : un système qui se branche sur l'existant, pas un chantier informatique.
Votre RSSI	PAGES 06 - 07	Les quatre principes de sécurité, la chaîne technique attestée de bout en bout et les preuves vérifiables en temps réel.
Votre DPO	PAGES 08 - 09	La qualification RGPD (article 28), le DPA, les sous-traitants ultérieurs et le positionnement au regard de l'IA Act.
Vous	PAGES 10 À 12	Les dix objections types et leurs réponses courtes, la checklist de due diligence et l'email prêt à transmettre à vos interlocuteurs.

LE RÉFLEXE À ÉVITER

Porter seul les questions techniques.

Défendre l'architecture, la sécurité et le RGPD à la place de l'éditeur vous met en position d'expert sur un sujet qui n'est pas le vôtre. Chaque question restée sans réponse coûte une à deux semaines de cycle.

NOTRE RECOMMANDATION

Transmettre, puis nous connecter.

Remettez à chacun sa section, puis mettez vos interlocuteurs en relation directe avec nous : nous répondons aux DSI, aux RSSI et aux DPO, et nous complétons les questionnaires sécurité. C'est notre travail, pas le vôtre.

CE QUE VOTRE COMITÉ DE DIRECTION DOIT SAVOIR

La question n'est plus d'autoriser l'IA. C'est de la gouverner.

Vos acheteurs utilisent déjà l'IA générative : rédaction de cahiers des charges, analyse d'offres, courriers fournisseurs. Souvent sur des comptes personnels, avec des données réelles, hors de tout cadre. Ce phénomène porte un nom, le **shadow AI**, et il transforme une opportunité en risque silencieux.

LES TROIS RISQUES DU STATU QUO

CE QUE LE SHADOW AI COÛTE DÉJÀ

Fuite de données

Prix, contrats, stratégies de négociation collés dans des outils grand public : sans DPA, sans hébergement maîtrisé, sans traçabilité, souvent depuis des comptes personnels.

Non-conformité passive

Aucun registre de traitement, aucun cadre contractuel, aucune supervision : l'entreprise porte le risque RGPD sans même le savoir.

Valeur dispersée

Chacun bricole ses prompts dans son coin : rien ne se capitalise, les livrables restent hétérogènes, invérifiables et impossibles à comparer entre acheteurs.

LE PIÈGE

Interdire, c'est pousser vers l'invisible.

Une interdiction ne supprime pas l'usage : elle le déplace vers des comptes personnels, hors de portée de la DSI. Le risque augmente à mesure que la visibilité disparaît.

NOTRE CONVICTION

Un cadre gouverné vaut mieux qu'une interdiction contournée.

Cortex × Impact³ apporte ce cadre : hébergement UE, comptes nominatifs, traçabilité, charte d'entreprise et méthode commune. Le même usage, sous contrôle, et enfin capitalisé.

LA VALEUR SE PROUVE AVANT TOUT ENGAGEMENT

GO / NO-GO À CHAQUE ÉTAPE

01
Démo sur cas réel

GRATUIT · SOUS NDA

Cortex × Impact³ démontré sur l'un de vos propres dossiers, avec vos données : livrables réels et estimation des gains, sans engagement.

02
Pilote cadré

290 € / MOIS / UTILISATEUR

La valeur validée en conditions réelles sur une catégorie maîtrisée, avec bilan chiffré et business case de déploiement.

03
Élargissement

SUR MESURE · DÉGRESSIF

Déploiement à l'ensemble de la fonction Achats, au rythme de vos équipes : chaque étape prouve la suivante.

UN SYSTÈME QUI SE BRANCHE, PAS UN CHANTIER

À TRANSMETTRE À VOTRE DSI

Indépendant de votre SI. Souverain sur vos données.

Cortex × Impact³ est un SaaS accessible par navigateur : aucune installation locale, aucun remplacement d'outil, aucun accès direct à vos systèmes au démarrage. Chaque brique de la chaîne est nommée, hébergée en Union européenne et couverte par des attestations vérifiables.

LA CHAÎNE TECHNIQUE, DE BOUT EN BOUT

CHAQUE MAILLON NOMMÉ, HÉBERGÉ, ATTESTÉ

Application Cortex × Impact ³	Éditée par Swott, société française, et hébergée chez OVHcloud en Union européenne : ISO 27001, 27017, 27018 et 27701, HDS et SecNumCloud selon les offres.
Backend et base de données	Supabase , hébergement UE : SOC 2 Type II, chiffrement au repos et en transit, logs conservés 60 jours au plus, DPA disponible.
Couche IA	Anthropic , attestée SOC 2 Type II et ISO 27001:2022 : aucun entraînement de modèles sur les données API, option Zero Data Retention, DPA proposé.
Poste utilisateur	Navigateur web et comptes nominatifs avec rôles et permissions : aucune installation locale, aucun agent sur les postes, aucune extension requise.

LE PARCOURS D'UNE DONNÉE

DE VOTRE EXTRACTION AU LIVRABLE

01 Vous versez Extractions ERP, tableurs, documents : vos fichiers, tels quels, dans votre espace cloisonné. Aucun accès direct à vos systèmes.	02 Le système traite Chiffrement en transit (TLS 1.2+) et au repos, sur toute la chaîne : application, base de données et couche IA.	03 Le livrable sort Structuré sur Impact ³ , sourcé sur vos données, traçable de bout en bout : l'acheteur voit ce qui a servi à quoi.	04 Vous gardez la main Conservation limitée, export et suppression sur demande : vos données et vos livrables restent votre propriété.
---	--	---	--

CE QUI TRANCHE

Aucun remplacement d'outil, aucun déploiement local : **le système se branche sur l'existant, sans le remettre en cause.**

Démarrer sans projet. Sortir sans friction.

La montée en puissance suit la valeur prouvée, jamais l'inverse : le système démarre sur de simples extractions et ne se connecte à votre SI qu'au dernier niveau, quand vos équipes l'ont décidé. À chaque étape, vous restez réversibles.

CE QUE ÇA CHANGE POUR VOS ÉQUIPES IT

DU JOUR 1 À LA RÉVERSIBILITÉ

Démarrage	Création des comptes et des rôles, remise de la charte sécurité : aucune intégration requise, premiers livrables dès le premier jour.
Accès et traçabilité	Accès limités aux utilisateurs autorisés (rôles et permissions), traçabilité des actions sensibles, espaces et données cloisonnés par organisation.
Intégrations	Optionnelles et tardives : Cortex Connect (niveau 4) branche ERP et SRM quand la valeur est prouvée et que vos équipes l'ont décidé, sans remettre en cause l'existant.
Exploitation	SaaS opéré par Swott : mises à jour continues, aucun maintien en condition opérationnelle à votre charge, posture de sécurité consultable en temps réel via le Trust Center Vanta.
Réversibilité	Export et suppression sur demande, conservation limitée selon votre configuration : vos données et vos livrables restent la propriété de votre organisation, à tout moment.

LE PIÈGE CLASSIQUE

Attendre le grand schéma directeur IA.

Reporter tout usage à un futur socle IA global, c'est laisser le shadow AI prospérer pendant dix-huit mois. Le risque court, lui, dès aujourd'hui.

NOTRE APPROCHE

Prouver petit, encadrer tout de suite.

Un pilote cadré sur une catégorie, sous NDA, sans intégration : votre DSI garde un Go / No-Go à chaque étape et le système s'aligne sur votre gouvernance, pas l'inverse.

CE QUI TRANCHE

Le pilote se décide en semaines, pas en trimestres : aucun chantier SI n'est requis pour prouver la valeur.

Une sécurité qui se prouve, pas qui se déclare.

Chaque maillon de la chaîne est couvert par des attestations vérifiables. Le tableau ci-dessous reprend l'état exact de notre conformité : ce qui est acquis, ce qui est attesté, ce qui est en cours, sans survendre.

CONFORMITÉ ET ÉLÉMENTS DE PREUVE		ÉTAT EXACT, SANS SURVENDRE
Swott · RGPD	CONFORME	Rôles, sécurité, confidentialité, droits des personnes. DPA disponible selon le périmètre contractuel.
Swott · Trust Center	ACTIF (VANTA)	Posture de sécurité en temps réel, monitoring continu des contrôles, accès aux justificatifs.
Swott · ISO/IEC 27001	EN COURS	Démarche prête à l'audit. Audit de certification prévu en septembre 2026.
Hébergement · OVHcloud	UE / FRANCE	ISO 27001/27017/27018/27701, HDS et SecNumCloud selon les offres.
Backend · Supabase	UE	SOC 2 Type II, RGPD, chiffrement repos et transit. Logs conservés 60 jours au plus. DPA disponible.
Couche IA · Anthropic	ATTESTÉE	SOC 2 Type II et ISO 27001:2022. Pas d'entraînement sur les données API, option Zero Data Retention, DPA proposé.

VÉRIFIER EN TEMPS
RÉEL

Charte sécurité complète, pack due diligence (appel d'offres et questionnaires sécurité) et **Trust Center Vanta** disponibles sur demande ou en libre accès.

Vos données et livrables restent la propriété de votre organisation, Swott agit en sous-traitant au sens du RGPD. Transmettez-nous vos trames de questionnaires : leur complétion fait partie du pack, et vos équipes peuvent préférer un échange direct de 30 minutes, preuves à l'écran.

UN CADRE ARTICLE 28, PAS UNE ZONE GRISE

À TRANSMETTRE À VOTRE DPO

RGPD : des rôles clairs, un cadre contractuel complet.

Votre organisation reste responsable de traitement : Swott agit exclusivement comme sous-traitant au sens de l'article 28 du RGPD, dans un cadre contractuel documenté et une chaîne de sous-traitance courte, listée et hébergée en Union européenne.

LE CADRE EN CINQ POINTS

DE LA QUALIFICATION AUX DROITS DES PERSONNES

Qualification	Votre organisation est responsable de traitement , Swott est sous-traitant : rôles, instructions et responsabilités formalisés dans le DPA, disponible selon le périmètre contractuel.
Données traitées	Essentiellement des données Achats : dépenses, offres, fournisseurs, contrats. Les données personnelles se limitent pour l'essentiel aux comptes utilisateurs et aux contacts professionnels présents dans vos documents.
Sous-traitants ultérieurs	Une chaîne courte et documentée : OVHcloud (hébergement, UE/France), Supabase (backend, UE), Anthropic (couche IA, attestée). Liste tenue à jour et remise avec le DPA.
Hébergement	Application et données hébergées en Union européenne. Aucun entraînement de modèles sur vos données, option Zero Data Retention sur la couche IA.
Droits et conservation	Conservation limitée, export et suppression sur demande, selon votre configuration : de quoi répondre aux demandes d'exercice de droits sans dépendre de votre prestataire.

POUR VOTRE REGISTRE

Un traitement documenté d'emblée.

Finalité, catégories de données, destinataires, durées, sous-traitants : le DPA et la charte sécurité vous donnent les éléments nécessaires à l'inscription au registre des traitements, dès le pilote.

NOTRE ENGAGEMENT

Vos données restent vos données.

Vos contenus et vos livrables restent la propriété de votre organisation. Nous ne les exploitons à aucune autre fin que le service : pas de revente, pas de mutualisation, pas d'entraînement de modèles.

RÈGLEMENT (UE) 2024/1689 · IA ACT

À TRANSMETTRE À VOTRE DPO

IA Act : un usage professionnel, supervisé par conception.

Le règlement européen sur l'IA s'applique de façon échelonnée depuis 2025. Voici comment Cortex × Impact³ se positionne, et ce que nous mettons à votre disposition pour documenter votre propre conformité.

LE POSITIONNEMENT EN QUATRE POINTS

RÈGLEMENT (UE) 2024/1689

Classification	Cortex × Impact ³ est un système d'IA à usage professionnel d'aide à la production et au pilotage de livrables Achats : il ne relève ni des pratiques interdites, ni des cas à haut risque listés à l'annexe III (<i>analyse à confirmer avec votre conseil selon vos cas d'usage</i>).
Supervision humaine	Par conception : l'acheteur formule, valide et décide, Cortex produit. Toute hypothèse manquante est signalée comme hypothèse à confirmer, jamais présentée comme un fait.
Transparence	Les livrables sont traçables de bout en bout : sources, données mobilisées et contributions des agents restent visibles et vérifiables par l'utilisateur.
Littératie IA (article 4)	L'obligation de formation des utilisateurs est couverte : l'onboarding et la Swott Academy structurent la montée en compétence de vos équipes sur l'usage professionnel de l'IA.

LE CALENDRIER D'APPLICATION, EN BREF

ENTRÉE EN VIGUEUR : AOÛT 2024

FÉVR. 2025	AOÛT 2025	AOÛT 2026	AOÛT 2027
Interdictions	Modèles généraux	Haut risque	Produits réglementés
Pratiques prohibées et obligation de littératie IA (article 4) applicables.	Obligations des fournisseurs de modèles d'IA à usage général.	Principales obligations des systèmes à haut risque de l'annexe III.	Systèmes d'IA intégrés à des produits soumis à réglementation sectorielle.

CE QUE ÇA CHANGE
POUR VOUS

Un déploiement documenté vaut mieux qu'un usage subi : Cortex fournit la traçabilité et la formation que l'IA Act attend des organisations.

Synthèse informative établie en juillet 2026 : elle ne remplace pas l'analyse juridique de votre organisation.

LES RÉPONSES PRÊTES À L'EMPLOI

Dix objections, dix réponses courtes.

Les mêmes questions reviennent partout. Voici les réponses factuelles, à reprendre telles quelles en réunion : chacune renvoie à une preuve documentée dans ce pack.

« Nos données vont entraîner des modèles. »	Non : aucun entraînement sur les données API, attesté par Anthropic, option Zero Data Retention et DPA à l'appui.
« Encore un cloud hors d'Europe. »	Application et données hébergées en Union européenne (OVHcloud France, Supabase UE), éditeur français, sous-traitant au sens du RGPD.
« Nous avons déjà Copilot ou un module IA S2P. »	Les IA généralistes ne connaissent ni votre méthode, ni vos données Achats. Cortex est agentique dès l'origine, conçu sur le métier, et se branche sans remettre en cause l'existant.
« C'est un projet SI de plus. »	Aucune installation, aucune intégration au démarrage : le système fonctionne sur extractions et ne se connecte au SI qu'au niveau Cortex Connect, une fois la valeur prouvée.
« Qui accède à quoi ? »	Comptes nominatifs, rôles et permissions, traçabilité des actions sensibles, espaces cloisonnés par organisation.
« Et si nous arrêtons ? »	Export et suppression sur demande, conservation limitée : vos données et vos livrables restent votre propriété.
« L'IA invente. »	Toute hypothèse manquante est signalée comme hypothèse à confirmer, jamais présentée comme un fait : l'acheteur garde la main et la décision.
« La sécurité se prouve, elle ne se déclare pas. »	Exactement : Trust Center Vanta en temps réel, charte sécurité complète, questionnaires complétés et audit ISO/IEC 27001 prévu en septembre 2026.
« Le RGPD est-il couvert ? »	Article 28, DPA, sous-traitants ultérieurs listés, hébergement UE : le dossier complet figure en pages 08 et 09 de ce pack.
« Et l'IA Act ? »	Usage professionnel hors des cas à haut risque de l'annexe III, supervision humaine par conception, littérature IA couverte par l'onboarding (page 09).

LA RÈGLE D'OR

Ne débattiez pas : transmettez la section concernée, puis proposez l'échange direct avec nous.

TROIS ÉTAPES, QUINZE JOURS

L'email est prêt. Le parcours aussi.

Tout est fait pour que la validation avance en parallèle de la démonstration de valeur, pas après elle. Trois étapes suffisent, et la première ne vous demande que deux minutes.

01

Transmettez

JOUR 1

Envoyez ce pack à votre DSI et à votre DPO avec l'email ci-dessous. Le NDA peut être signé dès ce stade.

02

Connectez

SEMAINE 1

Un échange de 30 minutes entre vos équipes et nous : architecture, sécurité et RGPD traités en direct, questionnaires pris en charge.

03

Prouvez

SEMAINE 2

Démonstration sur l'un de vos dossiers réels, sous NDA : la valeur se démontre pendant que la conformité se valide.

MODÈLE D'EMAIL · À COPIER TEL QUEL

DESTINATAIRES : DSI · DPO

Objet : Validation sécurité et conformité · Cortex x Impact³ (Swott)

Bonjour [prénom],

Nous étudions **Cortex x Impact³**, un système d'IA agentique dédié aux Achats, édité par Swott (société française). Avant d'aller plus loin, j'aimerais votre regard sur le volet sécurité et conformité.

Vous trouverez en pièce jointe leur dossier de validation : architecture et hébergement (UE), sécurité, RGPD et IA Act, avec les preuves associées (Trust Center, DPA, attestations). Trois points pour cadrer la lecture : les données sont hébergées en Union européenne et ne servent pas à entraîner de modèles ; Swott agit comme sous-traitant RGPD, DPA à l'appui ; le démarrage ne demande aucune intégration à notre SI.

Swott propose un échange direct de 30 minutes avec vous et prend en charge nos questionnaires sécurité. Pouvez-vous me partager vos disponibilités cette semaine ou la suivante ?

Merci d'avance,
[signature]

**Planifier l'échange DSI ·
DPO**

swott.fr · +33 5 82 88 03 05

GRATUIT · SOUS NDA · SANS ENGAGEMENT · RÉPONSE SOUS 24 H
OUVRÉES

TOUT CE QUE VOS ÉQUIPES PEUVENT EXIGER

La checklist due diligence, et qui s'en charge.

Voici la liste des éléments que vos équipes IT, sécurité et conformité sont en droit de demander, et la façon dont nous y répondons. Un principe : c'est à l'éditeur de produire ces preuves, pas à vous.

LA CHECKLIST COMPLÈTE

DOCUMENT · STATUT · CONTENU

NDA	DÈS LE 1ER ÉCHANGE	Vos données et vos dossiers restent confidentiels et votre propriété, avant toute démonstration.
Charte sécurité complète	REMISE	Architecture, chiffrement, gestion des accès, conservation, réversibilité : le document de référence pour votre RSSI.
DPA · accord de traitement	DISPONIBLE	Article 28, instructions documentées, sous-traitants ultérieurs, assistance à l'exercice des droits, selon le périmètre contractuel.
Trust Center Vanta	LIBRE ACCÈS	Posture de sécurité en temps réel et justificatifs : votre DSI vérifie par elle-même, sans nous demander la permission.
Questionnaires sécurité	NOUS COMPLÉTONS	Transmettez-nous vos trames (annexe d'appel d'offres, questionnaire DSI, grille RSSI) : leur complétion fait partie du pack due diligence.
Attestations de la chaîne	SUR DEMANDE	OVHcloud (ISO 27001/27017/27018/27701, HDS, SecNumCloud selon offres), Supabase (SOC 2 Type II), Anthropic (SOC 2 Type II, ISO 27001:2022).

UN SEUL RÉFLEXE

Ne répondez jamais vous-même à un questionnaire sécurité : **transmettez-le nous, nous nous en chargeons.**

Le NDA se signe dès le premier échange et chaque demande reçoit une réponse sous 24 h ouvrées : la due diligence ne doit jamais être ce qui ralentit votre projet.

Simplifier la complexité pour libérer votre performance Achats.



Planifier l'échange avec votre DSI et votre DPO

www.swott.fr · +33 5 82 88 03 05

LA FRENCH TECH

ENTREPRISE À MISSION

COMMUNAUTÉ DU COQ VERT