Europrivacy™® Academy
GDPR Audit and Certification Courses

Europrivacy Academy

Cours de mise en œuvre

www.academy.europrivacy.com

Europrivacy Academy

Europrivacy Cours de mise en œuvre

v.3 de 2025

À propos d'Europrivacy

Europrivacy est un Schéma de Certification développé pour évaluer et certifier la conformité du traitement des données avec le Règlement Général européen sur la Protection des Données (RGPD) et les réglementations nationales complémentaires. Il a reçu l'aval du Comité Européen de la Protection des Données (EDPB) en tant que label européen de protection des données applicable dans toutes les juridictions de l'UE.

Europrivacy permet une évaluation fiable et systématique de la conformité aux principes ISO. Il est facilement extensible aux réglementations complémentaires et aux technologies émergentes. Il fournit une méthodologie efficace pour réaliser des audits internes, pour identifier les non-conformités résiduelles et pour préparer le traitement des données à la certification. Il peut être utilisé par les Délégués à la Protection des Données (DPO), les auditeurs internes, les consultants et les organismes de certification.

Europrivacy est maintenu et supervisé par le Conseil International d'Experts en protection des données d'Europrivacy afin de le mettre à jour en fonction de l'évolution de la jurisprudence sur la protection des données personnelles, y compris les publications de l'EDPB. Europrivacy est géré administrativement par le Centre européen pour la certification et la protection de la vie privée (ECCP) au Luxembourg et est appliqué par des organismes de certification qualifiés, ainsi que par des cabinets d'avocats et des sociétés de conseil pour aider leurs clients à se conformer aux réglementations sur la protection des données.

À propos de l'Académie Europrivacy

L'Europrivacy Academy propose des cours de formation aux personnes souhaitant obtenir une qualification officielle en tant qu'experts en matière d'Europrivacy. L'Europrivacy Academy se concentre sur la méthodologie et les règles du Schéma de Certification Europrivacy. Il est supposé que les étudiants sont déjà familiarisés avec les réglementations en matière de protection des données. Les cours de l'Académie Europrivacy offrent une expérience d'apprentissage personnalisée à une grande variété de professionnels intéressés.

À propos du manuel

Le manuel du cours de mise en œuvre d'Europrivacy de l'Europrivacy Academy est un document complémentaire fourni aux participants du cours de mise en œuvre d'Europrivacy de l'Europrivacy Academy. Ce manuel est destiné à fournir un support complémentaire et un résumé du processus de certification, du rôle des Responsables de la Mise en Œuvre et des critères d'Europrivacy. Comme il est nécessaire de réussir l'examen pour obtenir une certification d'expertise, le manuel fournit un examen blanc qui peut familiariser les étudiants avec le type d'examen et le type de questions auxquels ils doivent se préparer.

Introduction

Le Schéma de Certification Europrivacy définit une méthodologie claire et efficace pour évaluer et certifier officiellement la conformité des activités de traitement des données avec le règlement général sur la protection des données (RGPD) et d'autres obligations complémentaires nationales et/ou spécifiques à un domaine. Il s'applique à un large éventail d'activités de traitement des données, depuis les processus et les services jusqu'aux systèmes de gestion de la protection des données.

Après avoir suivi le cours d'introduction, vous êtes déjà familiarisé avec le cadre général des certifications GDPR et le Schéma de Certification Europrivacy. Le cours de mise en œuvre et le présent manuel vous permettront d'approfondir votre compréhension du fonctionnement du processus de certification, y compris le rôle des Responsables de la Mise en Œuvre.

Le **premier chapitre** explique le rôle des Responsables de la Mise en Œuvre dans le processus de certification Europrivacy et détaille la procédure de maintien et de renouvellement des certifications. Il détaille également la procédure pour les appels et les plaintes. Le **deuxième chapitre** porte sur les règles relatives à la gestion des informations, y compris l'utilisation des certificats et des marques de conformité. Le **troisième chapitre** donne un aperçu détaillé des listes de critères, de vérifications et de contrôles d'Europrivacy, y compris leur demande et la spécification de la Cible d'Évaluation. Le manuel se termine par une section destinée à préparer les candidats à l'examen final par un examen blanc de 25 questions.

Toute référence à un document doit être comprise comme une référence à sa dernière version. Lorsqu'une nouvelle version d'un document est publiée, elle remplace toutes les versions précédentes du même document à la date de la publication ou à la fin de la période de transition. Les processus de certification et d'audit doivent utiliser la dernière version disponible du Schéma de Certification Europrivacy et des documents connexes à la date de début du processus. Lorsque de nouvelles versions des documents sont publiées au cours d'un processus de certification et d'audit, la procédure de certification doit en tenir compte et, dans la mesure du possible, se conformer à cette nouvelle version. Néanmoins, un processus en cours peut être achevé selon la version officielle du moment où il a commencé.

En cas de doute sur la demande et/ou l'interprétation des exigences du Schéma de Certification, il convient de se référer à la dernière version du Schéma de Certification.

Les documents normatifs et informatifs spécifiques au Schéma de Certification restent sous le contrôle du Propriétaire du Schéma, assisté par son Conseil International d'Experts.

Les experts d'Europrivacy sont responsables de l'obtention de la dernière version des documents utilisés via le site web de la Communauté Europrivacy. Les documents fournis par l'intermédiaire de l'Académie Europrivacy sont strictement destinés à la formation et ne constituent pas un matériel officiel pour la réalisation d'activités de certification.

Table de matières

Processus de certification Europrivacy

Rôle des Responsables de la Mise en Œuvre

Dans l'écosystème d'Europrivacy, les Responsables de la Mise en Œuvre qualifiés travaillent pour des cabinets de conseil et aident les organisations à s'assurer qu'elles respectent en permanence les réglementations applicables en matière de protection des données. Les cabinets de conseil ne se contentent pas de préparer les Applicants à la certification de leurs activités de traitement des données, ils les soutiennent également tout au long du processus de certification et de la phase de maintenance.

L'objectif principal des cabinets de conseil est de réduire les risques juridiques et financiers pour les Applicants. Les Responsables de la Mise en Œuvre utilisent les critères d'Europrivacy pour identifier les lacunes potentielles et les non-conformités résiduelles auxquelles le Applicant doit remédier.

Les Responsables de la Mise en Œuvre peuvent également être des délégués à la protection des données, qui souhaitent valider et éventuellement certifier la conformité de leur traitement de données.

Comme nous l'avons vu précédemment, le rôle des Responsables de la Mise en Œuvre est double.

- D'une part, les Responsables de la Mise en Œuvre réduisent les risques juridiques et financiers en appliquant une évaluation systématique de la conformité.
- D'autre part, les Responsables de la Mise en Œuvre soutiennent la préparation et la documentation du traitement des données à certifier.

Les cabinets de conseil peuvent tirer parti de l'offre Europrivacy Welcome Pack pour fournir une assistance complète à leurs Applicants.

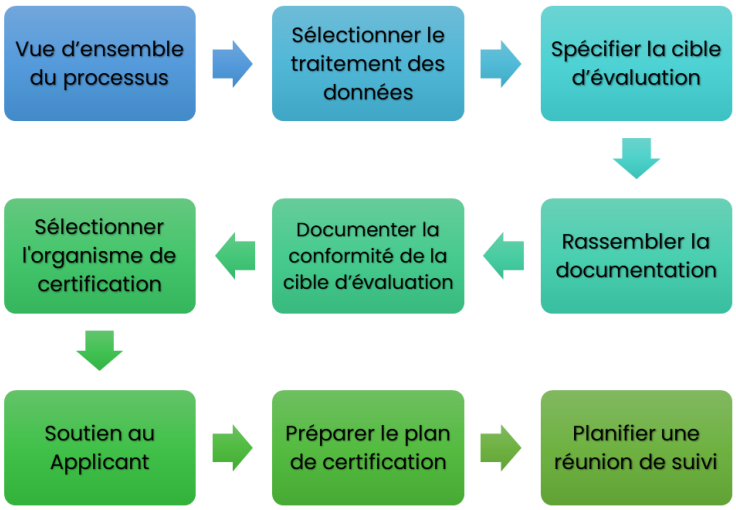


Figure 1 Parcours du Responsable de la Mise en Œuvre

Processus de préparation à Europrivacy

	ÉTAPE	SUJET	OBJECTIFS	RESSOURCES
1	Offre de bienvenue	Partenaire	Préparer une offre de bienvenue Europrivacy pour le Applicant	Présentation du Welcome Pack Europrivacy
2	Signature de l'offre	Applicant	Valider et signer l'offre	NA
3	Activate Welcome Pack	Partenaire	Activer le Welcome Pack pour le DPO du Applicant	Activation du Welcome Pack avec le soutien du ECCP
4	Sélectionner le traitement des données	Partenaire	Sélectionner avec le Applicant deux traitements de données prioritaires à préparer	NA
5	Préciser la Cible d'Évaluation	Partenaire	Préciser la cible de l'évaluation	A - Liste de contrôle de la demande et des Cibles d'Évaluation
6	Préparer la documentation	Partenaire	Préparer la documentation requise, y compris les inventaires et NOCAR	Lignes directrices à l'intention des Applicants ; D - Liste de contrôle de la documentation ; Modèles
7	Vérifier la conformité	Partenaire	Évaluer la conformité de la Cible d'Évaluation avec les critères, vérifications et contrôles d'Europrivacy	Critères G, C, T, vérifications et contrôles ; Lignes directrices sur l'utilisation des critères
8	Communiquer les lacunes identifiées	Partenaire	Dresser la liste des non-conformités identifiées et les communiquer au Applicant	Liste des non-conformités ; Modèle de rapport d'évaluation Europrivacy
9	Remédier aux non-conformités	Applicant	Traiter et résoudre les non-conformités identifiées	Liste des non-conformités
10	Valider la conformité	Partenaire	Vérifier et valider que les non-conformités ont été corrigées de manière adéquate	G, C, T Critères, vérifications et contrôles
11	Préparer la demande	Partenaire	Remplir et préparer la demande à soumettre à l'Organisme de Certification	Modèle de demande Europrivacy ; A - Liste de contrôle de la demande et des Cibles d'Évaluation
12	Demande de certification	Applicant	Sélectionner et demander à un Organisme de Certification de certifier les deux traitements de données sélectionnés	Formulaire de demande en ligne Europrivacy
13	Soutien à la certification	Partenaire	Soutenir le Applicant pendant le processus de certification	NA
14	Plan de certification	Partenaire	Élaborer un plan de certification pour les autres activités de traitement des données du Applicant	Modèle de plan de certification
15	Offre complémentaire	Partenaire	Faire une offre complémentaire pour le traitement des données restantes	NA
16	Réunion de clôture et prochaines étapes	Partenaire	Présenter les résultats, recueillir les retours et présenter l'offre complémentaire	NA
17	Signature de la nouvelle offre	Applicant	Valider et signer la nouvelle offre	NA

Maintien, renouvellement et recours

Maintien des certifications

En vertu des articles 42 et 43 du GDPR, des mesures de contrôle régulières sont obligatoires pour maintenir la certification pendant la période de contrôle. La période de contrôle de chaque certification doit être documentée. En principe, la certification Europrivacy devrait être accordée pour des périodes renouvelables de trois ans, commençant à la date de la certification la plus récente et se terminant à la date d'expiration de la certification.

Au cours de cette période, le Applicant doit s'assurer que sa Cible d'Évaluation est conforme aux exigences et aux critères du Schéma de Certification et informer l'Organisme de Certification de tout changement ou de toute préoccupation concernant sa conformité. L'Organisme de Certification maintient la certification sur la base de la démonstration que le Applicant continue à se conformer aux exigences du Schéma de Certification. Les activités de contrôle et de surveillance doivent être entièrement soutenues par le Applicant.

Le cycle de certification initial commence à la date de la décision de certification et se termine à la date d'expiration de la certification. Les certifications et recertifications réussies doivent être suivies de :

- un premier audit de surveillance dans les 12 mois suivant la date de certification.
- un deuxième audit de surveillance dans les 24 mois suivant la date de certification.
- le cas échéant, un audit de recertification dans les 36 mois suivant la date de certification.

Une recertification réussie avant la fin de la période de certification ouvre un nouveau cycle de 36 mois pour la certification. Si la décision de recertification est adoptée au cours des trois derniers mois précédant la date d'expiration du certificat précédent, la date de début du nouveau certificat peut être fixée à la date suivant la date d'expiration du certificat précédent.

Les activités de surveillance sont effectuées pour déterminer si la Cible d'Évaluation du Applicant continue à se conformer aux exigences du Schéma de Certification. La fréquence de l'audit peut augmenter en fonction de la capacité du Applicant certifié à se conformer aux exigences.

Les modifications apportées à la réglementation applicable en matière de protection des données, telles que les révisions législatives, les décisions des tribunaux nationaux ou supranationaux, les décisions de l'EDPB ou les décisions de la Commission européenne, sont suivies et traitées par l'Organisme de Certification. Si ces changements ont un impact sur les certifications délivrées, l'Organisme de Certification.

- Évalue le niveau d'impact sur la validité de la certification.
- Élabore un plan d'action.
- Contacte l'autorité compétente en matière de protection des données et demande la validation du plan d'action proposé.

- Met en œuvre le plan d'action après son approbation par l'Autorité de Protection des Données.

Recertification

Les certificats Europrivacy ont une durée de vie de trois ans et doivent faire l'objet d'une évaluation de recertification pour être renouvelés. L'Organisme de Certification décide du renouvellement d'une certification en fonction des résultats de l'audit de recertification, ainsi que des résultats de l'examen du schéma au cours de la période de certification et des plaintes reçues de la part des utilisateurs de la certification. L'objectif d'un audit de recertification est de confirmer la conformité continue de la Cible d'Évaluation avec les exigences d'Europrivacy.

Appels et plaintes

Le Applicant peut faire appel d'une décision auprès de l'Organisme de Certification, ou l'Organisme de Certification auprès du Propriétaire du Schéma, quel que soit celui qui a pris la décision.

Un tiers estimant qu'un processus de traitement des données certifié n'est pas conforme au Schéma de Certification ou à la réglementation applicable en matière de protection des données peut déposer une plainte auprès du Applicant certifié, de l'Organisme de Certification ou de l'autorité compétente.

En fonction des preuves communiquées, la partie destinataire doit informer l'Organisme de Certification et/ou l'Autorité de Protection des Données. Si les informations révélées par la plainte peuvent avoir un impact sur la confiance du public et la réputation du Schéma de Certification, le Propriétaire du Schéma en est informé sans délai.

Si la plainte n'a pas été correctement traitée par l'Organisme de Certification, la partie plaignante est invitée à en informer le Propriétaire du Schéma.

L'Organisme de Certification et ses employés sont responsables de l'enregistrement de toutes les plaintes et de tous les appels reçus, ainsi que des actions qui en découlent. Dès réception d'une plainte ou d'un appel relatif aux activités de certification, l'Organisme de Certification:

- accuse réception d'une plainte ou d'un appel formel
- rassemble et vérifie toutes les informations pertinentes
- notifie officiellement le résultat de la procédure au plaignant ou au requérant
- prend toute mesure ultérieure nécessaire pour résoudre la plainte ou le recours
- informe le Propriétaire du Schéma de tout problème majeur susceptible de constituer un risque pour le Schéma de Certification ou pour sa réputation

Lorsque des plaintes sont jugées valables, l'Organisme de Certification doit les traiter de manière appropriée et faire un effort raisonnable pour les résoudre. Le Applicant et l'Organisme de Certification doivent apporter leur soutien total pour enquêter et fournir des

clarifications afin de traiter et de résoudre la plainte. Une plainte bien fondée peut conduire à la suspension ou au retrait du certificat.

Afin de garantir une procédure impartiale, les décisions relatives à une plainte ou à un recours sont adoptées par des personnes qui.

- n'ont pas été directement impliqués dans le processus de certification concerné
- n'a pas fourni de services à la partie plaignante ou au Applicant certifié

Gestion de l'information et de la confidentialité

Gestion de l'information et de la confidentialité

L'Organisme de Certification doit disposer d'une méthodologie de documentation standardisé. La documentation produite au cours de l'évaluation doit se concentrer sur trois aspects principaux :

- La consistance et la cohérence des méthodes d'évaluation mises en œuvre.
- L'adéquation des méthodes visant à démontrer la conformité de la Cible d'Évaluation avec les critères de certification et donc avec le règlement relatif à la protection des données.
- L'impartialité du processus de décision.

Les organismes de certification doivent utiliser une méthodologie et un processus clairs et cohérents pour classer et identifier la documentation afin de garantir que le processus de certification est fiable et bien spécifié, ainsi que clair et convivial. La classification et l'identification de la documentation officielle du Schéma de Certification suivent les lignes directrices spécifiées dans le document *Management and Classification of Europrivacy Documents*. Tout document révisé est publié avec un numéro de version incrémenté.

En ce qui concerne la documentation fournie par le Propriétaire du Schéma, les processus de certification et d'audit doivent utiliser la dernière version disponible du Schéma de Certification et des documents connexes disponibles à la date de début du processus. Lorsque de nouvelles versions de documents sont publiées au cours d'un processus de certification et d'audit, celui-ci doit en tenir compte et, dans la mesure du possible, se conformer aux exigences de la nouvelle version.

L'Organisme de Certification est responsable de la gestion et de la protection adéquates des informations collectées ou générées au cours du processus de certification.

Tout le personnel impliqué dans les activités de certification ou ayant accès aux informations internes doit préserver et protéger la confidentialité de toutes les informations confidentielles liées à la certification. Par défaut, toutes les informations fournies par le Applicant ou liées au Applicant et à sa certification sont traitées comme des informations confidentielles, sauf si l'information.

- est accessible au public
- est qualifiée de non confidentielle par le Applicant
- est divulguée avec l'accord du Applicant et/ou
- doit être divulguée pour des raisons légales ou contractuelles.

La confidentialité ne s'applique pas aux informations qui doivent être publiées dans le registre des certifications et n'empêche pas l'accès légitime aux informations par des parties autorisées telles que les autorités de protection des données. L'Organisme de Certification peut être tenu par la loi de divulguer des informations confidentielles et doit se conformer à ces demandes. L'Autorité Nationale de Protection des Données et le

Propriétaire du Schéma peuvent demander l'accès à des informations confidentielles pour exercer leurs fonctions, telles que la surveillance et le traitement des plaintes relatives aux certifications. Seules les personnes autorisées, ayant l'obligation formelle et contractuelle de préserver la confidentialité des informations, doivent avoir accès aux données et aux fichiers stockés.

L'Organisme de Certification doit disposer de règles claires régissant la divulgation d'informations publiques sur ses plateformes de communication.

Par défaut, l'Organisme de Certification rend publiques des informations générales sur l'Organisme de Certification :

- Processus d'évaluation de la certification.
- Processus de décision relatif à la certification et à son champ d'application.
- Les types de systèmes de gestion et les schémas de certification dans lesquels elle opère.
- L'utilisation du nom, du logo et de la marque de conformité de l'Organisme de Certification.
- Procédures mises en place pour traiter les demandes d'information, les plaintes et les recours.
- La politique et le mécanisme d'impartialité.
- Les coordonnées de l'Organisme de Certification, telles que l'adresse postale.
- La politique de protection des données personnelles de l'Organisme de Certification et une procédure pour contacter son Délégué à la Protection des Données personnelles (DPO).

Sur demande, l'Organisme de Certification doit fournir des informations complémentaires sur :

- Les zones géographiques dans lesquelles l'Organisme de Certification opère.
- Le statut d'une certification donnée.
- Le nom, le document normatif correspondant, le champ d'application et la situation géographique du Applicant certifié.
- Informations sur le Schéma de Certification.
- Une description des moyens par lesquels l'Organisme de Certification obtient un soutien financier et des informations générales sur les frais facturés aux Applicants.
- Une description des droits et des devoirs des Applicants.
- Informations sur les procédures de traitement des plaintes et des recours.

Le Propriétaire du Schéma est responsable de la gestion et de la supervision du site web officiel d'Europrivacy, avec le dépôt des documents de référence officiels, ainsi que le registre officiel en ligne des certificats Europrivacy délivrés. Les organismes de certification peuvent reproduire les informations publiques sur leur site web pour autant qu'elles soient cohérentes avec les informations fournies par le Propriétaire du Schéma. Les organismes de certification tiennent à jour les informations publiées dans le registre officiel des certificats Europrivacy et doivent éviter tout retard dans la mise à jour des informations. Les

organismes de certification agréés doivent fournir un lien depuis leur site web vers le registre Europrivacy des objets certifiés et le site web d'information publique.

Utilisation de marques de conformité, de licences et de certificats

Une fois que le processus de certification est terminé et que la certification délivrée est publiée dans le registre des certificats Europrivacy, les candidats certifiés peuvent commencer à utiliser le logo et la marque de conformité Europrivacy. Le logo Europrivacy et la marque de conformité sont la propriété du Propriétaire du Schéma. Ils ne peuvent être utilisés par le Applicant qu'après avoir été approuvés par l'Organisme de Certification et sous sa supervision. Les organismes de certification et les Applicants doivent se conformer aux règles du Schéma de Certification régissant l'utilisation des certificats et de la marque de conformité, ainsi qu'à ses règles et lignes directrices en matière de communication sur Europrivacy.

La marque de conformité.

- fournit des informations claires sur le Schéma de Certification et son champ d'application.
- empêche toute communication trompeuse concernant la portée de la certification.
- permet de remonter jusqu'à l'Organisme de Certification et à son registre.

Il ne doit y avoir aucune ambiguïté, dans la marque ou dans le texte qui l'accompagne, en ce qui concerne l'Organisme de Certification qui a accordé la certification ou l'étendue de la certification.

L'Organisme de Certification et le Propriétaire du Schéma ont le droit d'exercer un contrôle sur la propriété, l'utilisation et l'affichage des licences, des certificats, des marques de conformité et de tout autre mécanisme indiquant que le traitement des données est certifié par l'Organisme de Certification. Ils vérifient si des références incorrectes au Schéma de Certification ou une utilisation trompeuse des licences, des certificats, des marques ou de tout autre mécanisme peuvent être trouvées dans la documentation ou dans d'autres publicités.

Le ECCP est chargé de veiller à l'utilisation correcte et à l'intégrité de la marque, du logo, du sceau et des logos secondaires d'Europrivacy sur toutes les publications, les articles promotionnels et l'équipement, qu'ils soient produits par les partenaires d'Europrivacy ou par une agence extérieure.

Principes fondamentaux

Europrivacy rassemble quelques principes clés en matière d'utilisation de la marque.

- Toute utilisation de la marque Europrivacy et/ou ECCP nécessite une autorisation ou une licence écrite et explicite du ECCP.
- L'utilisation du terme Europrivacy et/ou du logo Europrivacy doit toujours être conforme aux lignes directrices spécifiées.

- Le ECCP n'autorise pas l'utilisation du nom ou du graphisme d'Europrivacy dans une annonce, une publicité, une publication ou un rapport qui pourrait…
    - impliquer l'approbation d'un produit ou d'un service non lié à Europrivacy ; ou
    - induire en erreur des tiers en ce qui concerne les certifications délivrées.
- La documentation d'Europrivacy et le matériel de communication fourni par le ECCP sont protégés par le droit d'auteur et ne peuvent être reproduits, copiés, diffusés, modifiés ou vendus sans l'autorisation écrite expresse du ECCP.
- Les tiers qui utilisent la marque Europrivacy doivent se conformer aux instructions reçues du ECCP.

Marque et logo Europrivacy

Figure 2 Europrivacy mark and logo

Le terme Europrivacy et le logo Europrivacy sont des marques internationales gérées par le ECCP. Les marques textuelles et visuelles sont déposées dans plusieurs juridictions, y compris aux États-Unis.

Le mot-symbole d'Europrivacy est Europrivacy.

Le logo d'Europrivacy est composé des lettres "E" et "P" en bleu, avec six étoiles jaunes, comme le montre l'image. Le monogramme est souvent associée aux symboles de la marque déposée et de la marque enregistrée, ainsi qu'à un texte complémentaire.

Le monogramme et le signet Europrivacy ne doivent pas être modifiés, transformés, brisés ou utilisés d'une manière qui pourrait être perçue comme une marque nouvelle ou différente. Le mot-symbole et le monogramme doivent être clairement affichés et visibles dans une zone d'espace libre qui les entoure.

Certificats

Les traitements de données certifiés peuvent recevoir un certificat Europrivacy, sous le contrôle et l'approbation de l'Organisme de Certification. Les certificats doivent inclure

- Le logo de l'Organisme de Certification et d'Europrivacy
- Nom du Applicant certifié
- Si le Applicant agit en tant que contrôleur des données, ou sous-traitant des données ou contrôleur conjoint des données
- Le cas échéant, le nom du ou des contrôleurs conjoints
- Description claire de la Cible d'Évaluation et de sa portée géographique
- Le cas échéant, les extensions appliquées
- Les dates de délivrance et d'expiration du certificat
- Identifiant unique du certificat délivré

- Mentionner "Informations détaillées sur" suivi du nom de domaine du site web du Schéma de Certification et du registre des certificats en ligne
- Nom et adresse de l'Organisme de Certification délivrant le certificat

Les certificats doivent être clairs et facilement compréhensibles par les Personnes Concernées. Il est préférable qu'ils ne dépassent pas une page.

Marque de conformité

Les activités de traitement de données certifiées peuvent porter la marque de conformité Europrivacy, sous le contrôle et l'approbation de l'Organisme de Certification. La marque de conformité comprend

- Logo Europrivacy.
- Identifiant unique de certification.
- Nom de domaine du site web du Schéma de Certification.

En outre, la marque de conformité peut inclure des extensions du champ de certification, comme le montre l'exemple.

Figure 3 Marque de conformité Europrivacy

Déclaration de conformité

Statement of Conformity
with the GDPR and Europrivacy

Applicant
COMPANYNAME.SA
123 Address street
1111 City, Country
declares under its sole responsibility that the following data processing is in conformity with the following requirements:

Certification

Target of Evaluation:	Personal data processing by the smart parking solution deployed on the municipal territory of the city ABC.
Normative Scope:	Europrivacy criteria, v. 05.03.2019
Certified on and until:	April 27 2019 – April 26 2022
Certificate ID:	83F4:A014
Detailed information at:	www.europrivacy.com
Certification Body:	CERTIFICATION.SA 567 Address street 2222 City, Country

Signature

Authorized representative:	Mr ABC
Date:	May 3 2019
Signature:	XXXXXX

Figure 4 Europrivacy Statement of conformity

Les Applicants peuvent inclure des déclarations de certification sur leur site web ou sur d'autres informations et documents pertinents, sous réserve de l'approbation écrite préalable de l'Organisme de Certification.

La déclaration comprend

- la référence à Europrivacy et, lorsqu'il est autorisé, le logo Europrivacy.
- le nom du Applicant certifié.
- le cas échéant, le nom du ou des responsables conjoints du traitement.
- une indication claire de la Cible d'Évaluation et de sa portée géographique.
- le cas échéant, une indication claire des normes ou exigences complémentaires qui ont été ajoutées.

- les dates de délivrance et de validité du certificat.
- l'identifiant unique du certificat délivré.
- la mention "Informations détaillées sur" suivie du nom de domaine du site web du Schéma de Certification et du registre des certificats en ligne.
- ainsi que le nom et l'adresse de l'Organisme de Certification qui délivre le certificat.

Lorsque la certification est délivrée sur une base volontaire sans que le Applicant n'en demande la validité au titre des articles 42 et 43 du GDPR, la déclaration de conformité doit l'indiquer clairement.

Autres considérations

Si un certificat, une déclaration ou une marque de conformité liée à une certification Europrivacy est affichée sur un support électronique, tel qu'une page web ou un document pdf, elle doit inclure un lien hypertexte direct vers la page d'accueil du Schéma de Certification ou vers la page spécifique de la Cible d'Évaluation certifiée dans le registre en ligne. Les marques de conformité, les certificats et les déclarations de certification ne doivent pas être utilisés d'une manière susceptible de créer une confusion ou une communication trompeuse concernant la Cible d'Évaluation de la certification référencée.

L'Organisme de Certification doit exercer un contrôle approprié de la propriété de l'utilisation et de la référence à ses certificats délivrés, et il doit prendre des mesures pour traiter les références incorrectes au statut de certification ou l'utilisation trompeuse des documents de certification, des marques ou des rapports d'audit. Ces mesures peuvent comprendre des demandes de correction et des actions correctives, la suspension, le retrait de la certification, la publication de la transgression et, si nécessaire, une action en justice.

Liste détaillée des critères, des vérifications et des contrôles

Critères, vérifications et contrôles d'Europrivacy

Critères d'évaluation

Les critères d'évaluation sont appliqués conformément à la dernière version des exigences du Schéma de Certification Europrivacy. L'Organisme de Certification applique les critères d'évaluation.

- Garder à l'esprit les droits des Personnes Concernées et les risques potentiels pour leurs données personnelles.
- De manière cohérente et homogène.
- De manière vérifiable et auditable.
- En tenant compte de la taille de l'organisation, de la nature du traitement des données, ainsi que des risques identifiés pour les données et les Personnes Concernées.

Les critères d'évaluation, les vérifications et les contrôles détaillés d'Europrivacy visent à évaluer les aspects suivants :

- Identification des données personnelles traitées.
- Conformité aux exigences relatives aux informations sur les activités de traitement des données fournies aux Personnes Concernées.
- Légalité du traitement et respect des exigences en matière de "consentement préalable en connaissance de cause".
- Respect des exigences relatives aux mineurs d'âge.
- Respect du principe de minimisation des données dès la conception et par défaut.
- Respect du principe de transparence tel que spécifié par le GDPR.
- L'analyse des flux de données personnelles, y compris les questions liées aux sous-traitants et au transferts transfrontaliers de données.
- Cycle de vie des données personnelles et minimisation des périodes de conservation des données personnelles.
- Mise en œuvre effective des droits de la Personne Concernée.
- Présence et conformité des données indirectes.
- Mise en œuvre de mesures appropriées pour protéger les droits, les libertés et les intérêts légitimes de la Personne Concernée dans le cadre de la prise de décision individuelle automatisée.
- Sécurité et protection efficace et intégrité des données collectées.
- Mise en œuvre par le contrôleur de mesures techniques et organisationnelles appropriées pour protéger les données.
- Si des sous-traitants sont utilisés, l'accord de procédures en place permet au contrôleur de s'assurer que leurs sous-traitants fournissent des garanties suffisantes pour mettre en œuvre des mesures techniques et organisationnelles appropriées.

- Lorsqu'ils sont inclus dans le champ d'application de la certification, les exigences et critères normatifs complémentaires nationaux et/ou spécifiques à un domaine.

Les critères d'évaluation sont traduits en listes détaillées de critères, de vérifications et de contrôles tenues par le Propriétaire du Schéma et mises à la disposition des autorités chargées de la protection des données et des tiers agréés. La liste des critères, des vérifications et des contrôles est utilisée par les organismes de certification pour évaluer systématiquement la conformité du traitement des données dans la Cible d'Évaluation.

Les critères, vérifications et contrôles d'Europrivacy sont disponibles sous diverses formes dans le Welcome Pack et sur le site web de la communauté Europrivacy. Les critères Europrivacy peuvent également être utilisés par le biais de logiciels et solutions d'évaluation de la conformité proposés par des partenaires qualifiés.

Critères fondamentaux

Au-delà des obligations fondamentales du GDPR, les Cibles d'Évaluation peuvent être soumises à des réglementations nationales complémentaires ou spécifiques à un domaine.

La liste de critères la plus importante est la suivante.

1. Les critères fondamentaux GDPR d'Europrivacy qui rassemblent les exigences du GDPR applicables à tous les traitements de données.

Il est complété par trois séries d'exigences complémentaires.

2. Vérifications et contrôles contextuels complémentaires pour évaluer la conformité avec les exigences spécifiques au domaine et à la technologie.
3. Mesures techniques et organisationnelles Vérifications et contrôles pour évaluer les mesures de sécurité mises en place pour protéger les données traitées.
4. Les obligations nationales en matière de protection des données avec leurs compléments de protection des données.

Exigences nationales et normatives complémentaires

Les certifications GDPR au titre de l'art. 43 du GDPR exigent que le traitement des données certifié soit conforme aux obligations nationales de l'UE du pays où le responsable du traitement des données ou le sous-traitant a son siège. Ces obligations comprennent également toutes les réglementations nationales spécifiques à un domaine liées à la protection des données personnelles qui sont applicables à la cible de l'évaluation. Chaque pays dispose de lois et de réglementations nationales distinctes qui ont un impact sur les exigences en matière de protection des données et les étendent. Le Applicant doit s'assurer que sa Cible d'Évaluation respecte les réglementations nationales applicables tout en surveillant leur révision.

Le Applicant postulant depuis l'Espace économique européen doit solliciter à un expert possédant les compétences juridiques adéquates d'évaluer la conformité de sa Cible

d'Évaluation avec les obligations nationales complémentaires qui dépassent les obligations du GDPR dans le pays de la demande. Les résultats de l'évaluation doivent être consignés dans un rapport écrit : le "*National Obligation Compliance Assessment Report" (NOCAR)*. En l'absence de NOCAR, l'Organisme de Certification peut également effectuer une évaluation de la conformité de la Cible d'Évaluation avec l'obligation nationale applicable dans le pays de la demande, sous réserve du même niveau d'exigences que pour le NOCAR.

Exigences en matière de mesures techniques et organisationnelles complémentaires

La certification Europrivacy exige que des mesures techniques et organisationnelles adéquates soient mises en place pour protéger les données traitées et stockées.

Les vérifications et contrôles des mesures techniques et organisationnelles complémentaires ont été spécifiés pour évaluer l'adéquation de la sécurité du traitement des données. Ces vérifications et contrôles complètent les critères fondamentaux et sont obligatoires pour toutes les Cibles d'Évaluation, sauf si la Cible d'Évaluation.

- est couvert par une certification ISO/IEC 27001 valide ; et
- n'effectue aucun traitement de données à haut risque.

Exigences complémentaires contextuelles et spécifiques au domaine

Les vérifications et contrôles contextuels complémentaires contiennent divers sous-ensembles de vérifications et de contrôles correspondant à des technologies ou à des domaines d'application spécifiques. L'Organisme de Certification applique et évalue tous les sous-ensembles de vérifications et de contrôles applicables aux activités de traitement des données incluses dans la Cible d'Évaluation.

Processus de certification

L'évaluation de la conformité à Europrivacy est organisée selon une séquence bien structurée de critères, de vérifications et de contrôles.

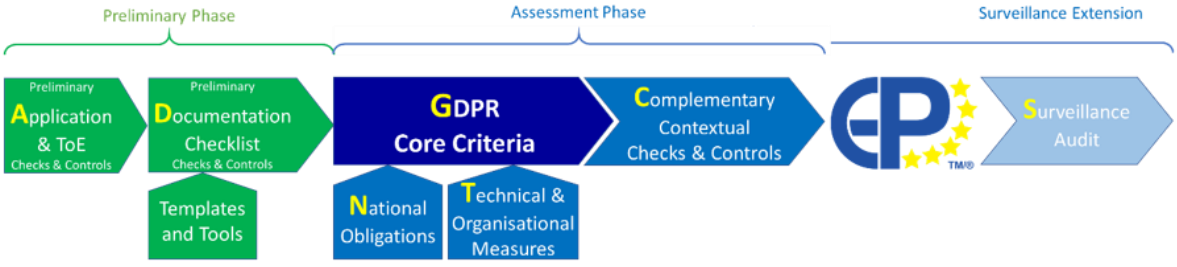


Figure 5 Processus de certification Europrivacy et vérifications et contrôles applicables

La phase préliminaire vise à s'assurer que la cible de l'évaluation est prête à être évaluée.

Les vérifications et contrôles de la demande et de la Cible d'Évaluation sont utilisés par l'Organisme de Certification pour évaluer l'adéquation de la spécification de la Cible d'Évaluation avec les lignes directrices établies par l'EDPB. Ces vérifications et contrôles

peuvent être préparés par le Applicant mais doivent être validés par l'Organisme de Certification avant le début du processus d'évaluation.

La liste de contrôle de la documentation vise à faciliter la collecte de la documentation et à garantir que l'équipe d'audit aura accès à la documentation requise. Elle doit être complétée par le Applicant puis validée par l'auditeur principal avant le début de l'évaluation.

L'adéquation de la Cible d'Évaluation et de la documentation disponible doit être validée par l'auditeur principal avant d'entamer le processus d'évaluation proprement dit.

Les vérifications et contrôles suivants sont utilisés pour évaluer la conformité de la Cible d'Évaluation avec Europrivacy. Le Applicant peut préparer des preuves pour satisfaire aux différents critères, mais la validation formelle est sous la responsabilité exclusive de l'Organisme de Certification.

Les critères fondamentaux GDPR constituent la base de tous les processus de certification d'Europrivacy et sont appliqués par les auditeurs de l'Organisme de Certification à chaque Cible d'Évaluation, quel que soit son domaine d'application et sa localisation. Les critères fondamentaux GDPR permettent une évaluation systématique de la conformité aux obligations contenues dans le GDPR. Ils garantissent que toutes les certifications Europrivacy assurent un niveau élevé de conformité avec le GDPR. Cette liste est obligatoire pour toutes les certifications.

Les vérifications et contrôles contextuels complémentaires sont spécifiés pour évaluer les exigences en matière de protection des données spécifiques à un domaine ou à une technologie. Ils prennent en compte les publications et les lignes directrices de l'EDPB et des autorités nationales chargées de la protection des données, ainsi que l'expertise de la communauté des chercheurs. Cette liste est obligatoire pour chaque certification. Les vérifications et contrôles contextuels complémentaires sont regroupés dans divers sous-ensembles de vérifications et de contrôles applicables à des technologies et à des domaines d'application spécifiques. L'Organisme de Certification doit parcourir la liste et doit évaluer et vérifier tous les sous-ensembles applicables à la Cible d'Évaluation.

La certification Europrivacy exige que des mesures techniques et organisationnelles adéquates soient mises en place pour protéger les données traitées. Les vérifications et contrôles des mesures techniques et organisationnelles visent à évaluer la conformité des mesures mises en place par le Applicant pour sécuriser et protéger les données traitées.

Europrivacy a spécifié quelques vérifications et contrôles complémentaires à appliquer lors des audits de surveillance ou de recertification pour évaluer les obligations spécifiques aux traitements de données déjà certifiés, telles que l'obligation de fournir des informations sur les traitements de données certifiés dans les langues des États membres.

Le modèle de liste des non-conformités doit être utilisé par l'Organisme de Certification pour signaler et énumérer les non-conformités identifiées auxquelles le Applicant doit

remédier pour être certifié. L'Organisme de Certification peut également utiliser ses propres modèles pour signaler les non-conformités.

Une liste de contrôle informative pour la publication du certificat est mise à la disposition de l'Organisme de Certification afin de s'assurer que toutes les exigences administratives sont satisfaites avant de délivrer un certificat Europrivacy.

ID	List of Checks and Controls	Status	Lead	Alternative	CF	CB
A	**Application and Target of Evaluation**	**Mandatory**	**CB**	**No**	**X**	**X**
I	Inventories to be completed or provided by the Applicant	Informative	Applicant	Data processing registry	X	X
D	**Documentation Validation**	**Informative**	**App. & CB**	**No**	**X**	**X**
E	Evaluation of Datasets	Informative	App. & CB	CB Management System	X	X
G	**GDPR Core Criteria**	**Mandatory**	**CB**	**No**	X	X
C	**Complementary and Contextual Checks and Controls**	**Mandatory**	**CB**	**No**	**X**	**X**
T	**Technical and Organisational Measures (TOM)**	**Mandatory**	**CB**	**ISO 27001/27701**	**X**	**X**
N	National requirements	Informative	CB	Legal assessment	X	X
S	**Surveillance Audits**	**Mandatory**	**CB**	**No**	**X**	**X**
NC	**List of Non-Conformities**	**Mandatory**	**CB only**	**CB Management System**		**X**
Z	Certificate Publication checklist	Informative	CB only	CB Management System		X

Figure 6 Applicabilité des contrôles et vérifications

Applicabilité spécifique

Les critères, vérifications et contrôles d'Europrivacy sont différenciés et liés à des catégories distinctes afin de déterminer et de faciliter leur applicabilité.

Une colonne indique si les critères, les vérifications et les contrôles sont applicables.

- Contrôleurs de données (C)
- Sous-traitant des données (P)
- Responsables du traitement des données et sous-traitants (CP)

Afin d'assurer la proportionnalité et de différencier les traitements de données simples des traitements plus importants et sensibles, une autre colonne différencie les critères, les vérifications et les contrôles dans les catégories suivantes.

- Obligatoire par défaut pour tous les processus de certification
- Elle n'est pas nécessaire pour certifier un traitement de données simple, mais elle est obligatoire pour certifier tout traitement de données à haut risque, défini comme un traitement de données qui...
  - traite des catégories particulières de données personnelles ou des données relatives à des condamnations pénales, ou
  - cible spécifiquement les données personnelles de mineurs d'âge, ou
  - est susceptible d'entraîner un risque élevé pour les droits et libertés des personnes physiques.
- La catégorie "Exemptions" permet de déterminer si une exemption à un critère requis peut être justifiée.

Une autre colonne précise si les critères, les vérifications et les contrôles sont.

- Spécifique à chaque traitement de données
- Générique et commun à plusieurs traitements de données

Une autre colonne précise si le critère est applicable aux importateurs de données basés en dehors de l'Espace économique européen qui ne sont pas directement soumis au GDPR.

- R indique que le critère est requis pour les importateurs de données basés en dehors de l'EEE.
- NR indique que le critère n'est pas requis pour les importateurs de données établis en dehors de l'EEE.

Format des critères

Les critères sont formulés sous forme de clauses impératives ("shall" clauses) qui s'articulent avec des connecteurs logiques claires en utilisant les mots "AND", "OR" et "IF...YES".

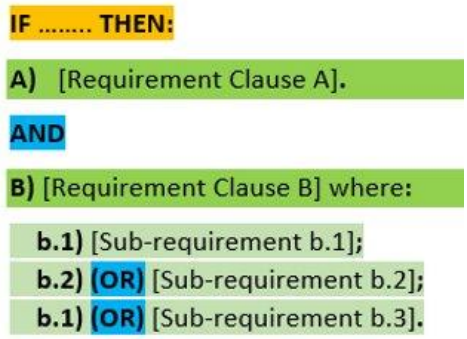


Figure 7 Format des critères

Conditional clauses permettent de restreindre l'applicabilité d'un critère à certaines conditions. Elles commencent par le mot "IF" et se terminent par "YES". Si les conditions sont applicables au traitement des données, les critères ultérieurs correspondants doivent être évalués. Si la condition ne s'applique pas, les critères suivants peuvent être ignorés.

Les critères sont spécifiés dans une ou plusieurs clauses spécifiant des exigences formelles, appelées **Requirement Clause**. Un critère peut contenir plusieurs clauses d'exigences. Chaque clause d'exigence majeure commence par une lettre en majuscule et une parenthèse.

Lorsque les critères comprennent plusieurs clauses d'exigences, un terme de **Boolean Relation** est spécifié entre chaque clause d'exigence.

Chaque clause majeure peut éventuellement contenir un ensemble de **Sub-requirements**. La liste des sous-exigences est précédée d'une colonne (" :"). Chaque sous-exigence.

- commence par la lettre de la clause correspondante de l'exigence majeure, suivie d'un point et d'un chiffre.
- inclut un terme de relation booléenne entre parenthèses, sauf pour la première sous-exigence de la liste.
- se termine par une demi-colonne si la sous-exigence est suivie d'une autre sous-exigence, ou par un point s'il s'agit de la dernière sous-exigence de la liste.

Spécifier la Cible d'Évaluation

La Cible d'Évaluation précise et délimite la portée des activités de traitement des données à caractère personnel à certifier. Elle doit être clairement spécifiée et compréhensible par

les tiers, y compris les Personnes Concernées. Une certification GDPR ne peut être délivrée au niveau d'une entreprise ou de son système de gestion dans son ensemble. Elle est considérée comme trop vaste et pas assez spécifique pour être efficace et fiable. Il convient plutôt de considérer les activités de traitement des données, telles que les bases de données clients, le service d'assistance à la clientèle, les services de paie et de comptabilité, le site web de l'entreprise ou une application mobile.

La spécification de la cible de l'évaluation offre une certaine souplesse et une certaine liberté. Il peut s'agir d'une ou de plusieurs opérations de traitement ayant des finalités distinctes. Toutefois, la Cible d'Évaluation doit présenter un certain niveau d'homogénéité en ce qui concerne la source des données traitées et l'objectif général de l'activité de traitement à certifier. Si la Cible d'Évaluation implique plusieurs juridictions et/ou entités juridiques, sa spécification doit être cohérente avec le contrôle effectif et la responsabilité des activités de traitement des données à certifier. Cela peut impliquer d'effectuer et de délivrer une certification en plusieurs segments.

L'Organisme de Certification devra évaluer chaque activité de traitement des données incluse dans la Cible d'Évaluation. La documentation de certification doit être absolument transparente et claire.

La Cible d'Évaluation doit être formellement spécifié avec une description claire de l'activité de traitement des données à caractère personnel à certifier. La spécification doit inclure des informations détaillées telles que la source des données, les catégories de données à caractère personnel, les catégories de Personnes Concernées, la finalité du traitement des données, les pays où le traitement a lieu, le recours à des sous-traitants, une description narrative du traitement, etc.

Le processus de spécification de la Cible d'Évaluation comprend 6 étapes principales.

1. **Sélectionner l'activité de traitement des données**. Commencez par les activités de traitement de données prioritaires, par exemple en termes de risque pour le Applicant.

2. **Spécifier et cartographier la Cible d'Évaluation**. Spécification et cartographie des flux de données personnelles dans la Cible d'Évaluation, à l'aide du formulaire de demande de certification Europrivacy.

3. **Vérifier l'adéquation de la Cible d'Évaluation** en appliquant le document "Demande et Cible d'Évaluation - Vérifications et contrôles préliminaires" afin de valider son exhaustivité et son adéquation.

4. **Documenter la conformité de la Cible d'Évaluation** en vérifiant et en documentant la manière dont les activités de traitement des données dans la Cible d'Évaluation sont conformes aux critères Europrivacy applicables. Cette étape permet déjà de réduire considérablement les risques.

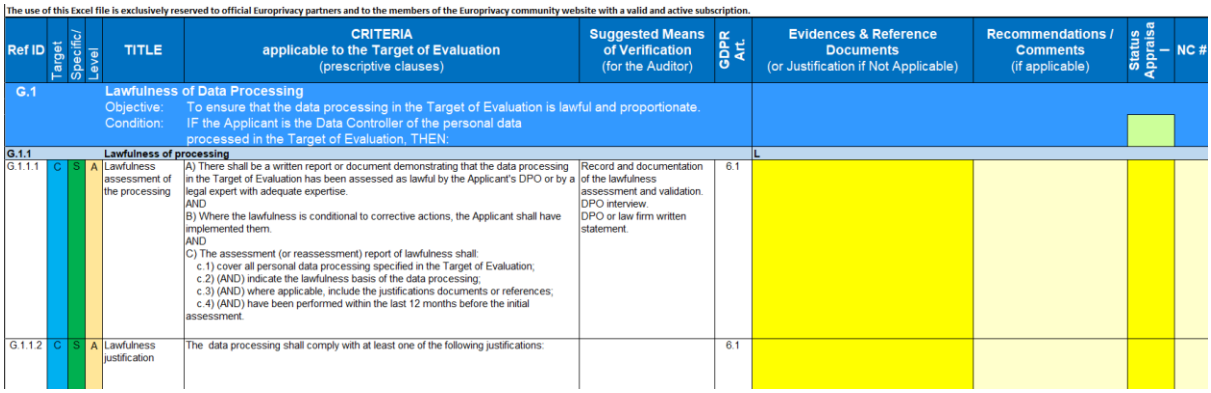
5. **Certifier la cible de l'évaluation**. Le certificat de conformité permettra au Applicant de démontrer, de valoriser et de communiquer sa conformité.

6. **Maintenir et apprécier la conformité**. Une fois certifié, le maintien de la conformité des activités de traitement des données s'appuie sur les ressources en ligne qui, entre autres fonctionnalités, fournissent également des notifications sur les changements réglementaires. Les audits de surveillance ultérieurs démontreront si le Applicant maintient sa conformité au fil du temps.

Structure du tableau et comment le remplir

Structure horizontale de la table

La liste est structurée en plusieurs onglets. L'onglet intitulé "Core GDPR" rassemble les critères, vérifications et contrôles fondamentaux qui sont abordés dans chaque audit.



The use of this Excel file is exclusively reserved to official Europrivacy partners and to the members of the Europrivacy community website with a valid and active subscription.

Ref ID	Target	Specific/ Level		TITLE	CRITERIA applicable to the Target of Evaluation (prescriptive clauses)	Suggested Means of Verification (for the Auditor)	GDPR Art.	Evidences & Reference Documents (or Justification if Not Applicable)	Recommendations / Comments (if applicable)	Status Appraisal	NC #
G.1				Lawfulness of Data Processing Objective: To ensure that the data processing in the Target of Evaluation is lawful and proportionate. Condition: IF the Applicant is the Data Controller of the personal data processed in the Target of Evaluation, THEN:							
G.1.1				Lawfulness of processing				L			
G.1.1.1	C	S	A	Lawfulness assessment of the processing	A) There shall be a written report or document demonstrating that the data processing in the Target of Evaluation has been assessed as lawful by the Applicant's DPO or by a legal expert with adequate expertise. AND B) Where the lawfulness is conditional to corrective actions, the Applicant shall have implemented them. AND C) The assessment (or reassessment) report of lawfulness shall: c.1) cover all personal data processing specified in the Target of Evaluation; c.2) (AND) indicate the lawfulness basis of the data processing; c.3) (AND) where applicable, include the justifications documents or references; c.4) (AND) have been performed within the last 12 months before the initial assessment.	Record and documentation of the lawfulness assessment and validation. DPO interview. DPO or law firm written statement.	6.1				
G.1.1.2	C	S	A	Lawfulness justification	The data processing shall comply with at least one of the following justifications:		6.1				

Chiffre 8 Structure horizontale du tableau

Le tableau Excel comprend les colonnes suivantes :

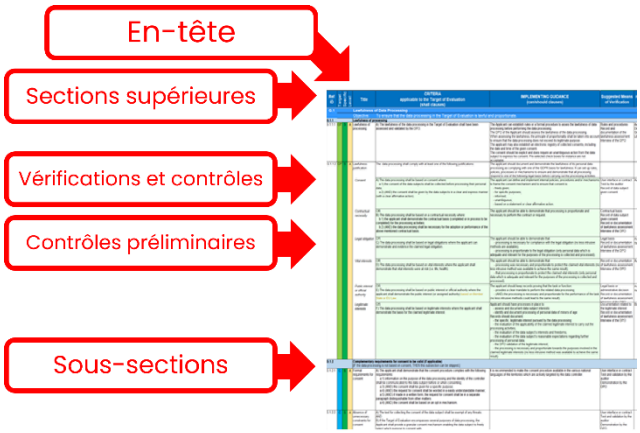
1. La colonne **Ref ID** fournit un identifiant unique et distinct pour chaque vérification et contrôle.
2. La colonne "**Cible**" indique à qui s'appliquent le contrôle et la vérification.
    - Contrôleurs uniquement.
    - Sous-traitants uniquement.
    - Les contrôleurs et les processeurs.
3. La colonne **Spécifique/Générique** précise si les vérifications et les contrôles sont spécifiques ou génériques.
4. La colonne **Niveau** indique le niveau des vérifications et des contrôles.
5. La colonne **Titre** indique le titre de la vérification et du contrôle.
6. La colonne **Critères** décrit l'exigence formelle à mettre en œuvre par le Applicant et à évaluer par l'auditeur. Les critères sont des clauses prescriptives que le Applicant doit respecter.
7. La colonne "**Moyens de vérification suggérés**" donne des indications à l'auditeur sur les sources habituelles où se trouvent les informations. Elle est indicative et les auditeurs peuvent choisir toute autre source d'information pertinente.

8. La colonne **Article du GDPR** fournit une indication du principal article du GDPR lié à la vérification et au contrôle.
9. La colonne **Preuves et documents de référence** doit être remplie par l'auditeur avec une indication claire des preuves qui ont été prises en compte pour déterminer la conformité ou la non-conformité. Ce champ est obligatoire, sauf pour les vérifications et les contrôles qui sont considérés comme non applicables à la certification.
10. La colonne **Recommandations/Commentaires** (le cas échéant) permet à l'équipe d'audit d'identifier certains problèmes ou éléments à traiter par le Applicant.
11. La colonne **Statut** est utilisée par l'auditeur pour qualifier le statut de la constatation sur le contrôle.
12. La colonne **NC #** sert à indiquer le numéro d'identification d'une non-conformité identifiée.

Les vérifications et les contrôles sont regroupés en différents critères conformément à la structure du GDPR.

Structure verticale de la table

1. **L'en-tête** indique le titre et la fonction de chaque colonne.
2. **Les sections supérieures** indiquent le début d'une section principale.
3. **Les sous-sections** indiquent le début d'une sous-section à l'intérieur d'une section principale.
4. **Les vérifications et les contrôles** sont identifiés par le fond blanc de leurs cellules dans la colonne Exigence obligatoire.
5. **Les contrôles préliminaires** sont identifiés par le fond vert clair de leurs cellules dans la colonne des exigences obligatoires.



Chiffre 9 Structure du tableau vertical

Processus global

La procédure suivante s'applique à l'évaluation des vérifications et des contrôles d'une section.

1. Effectuer les vérifications et contrôles requis dans la catégorie supérieure
2. Passer systématiquement en revue les vérifications et les contrôles
3. Effectuer les contrôles préliminaires

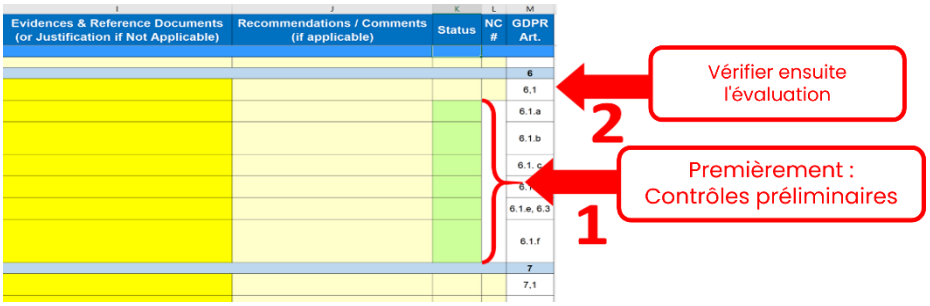


Figure 10 Processus global

Pour chaque vérification et contrôle

4. Fournir des preuves claires dans la cellule correspondante
5. Compléter par des commentaires et des suggestions ("Recommandations/commentaires")
6. Déterminer l'état de la vérification et du contrôle
7. Si une non-conformité est identifiée, l'inclure dans la colonne correspondante ("NC#") avec un identifiant clair (numéro ou lettre).
8. Un tableau de bord est fourni au bas du tableau, offrant un résumé de l'état des résultats des vérifications et des contrôles.

Code de statut		Signification/Explication	Tot	%
OK		Conformité : L'exigence a été **contrôlée** et semble être respectée. Aucune non-conformité n'a été identifiée.	2	22%
OK+		Bonnes pratiques allant au-delà de la simple conformité	2	22%
Obs		**Observation**	1	11%
			5	56%
NC Min		Une **non-conformité mineure** (non critique) a été identifiée.	1	11%
NC Maj		Une **non-conformité majeure** (critique) a été identifiée.	1	11%
?		**Information manquante/ne sait pas**	0	0%
NA		Le contrôle n'est pas applicable pour la certification visée	2	22%

Figure 11 Tableau de bord indicatif

Options de statut

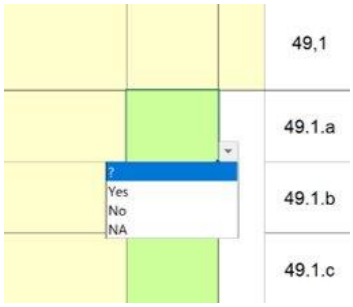
Le champ Statut dans les cellules jaunes propose une liste de plusieurs options, correspondant à différents statuts :

Chiffre 12 Cellules de statut régulier

Code d'état	Signification/Explication
?	Informations manquantes/ne sait pas
OK	Conformité : L'exigence a été contrôlée et semble être respectée. Aucune non-conformité n'a été identifiée.
OK+	Les bonnes pratiques dépassent la simple conformité
Obs	Observation
Min NC	Une non-conformité mineure (non critique) a été identifiée.
Maj NC	Une non-conformité majeure (critique) a été identifiée.
NA	Le contrôle **n'est pas applicable** pour la certification visée

Tableau 1 Options de statut

Certaines cellules correspondent à des questions complémentaires utilisées pour évaluer le statut d'un contrôle. La couleur d'arrière-plan des cellules correspondant au statut est verte et non jaune. Le champ Statut dans les cellules vertes offre une liste simplifiée d'options, correspondant à différents statuts.



Chiffre 13 Cellule d'état des sous-questions

Code d'état	Signification/Explication
?	Informations manquantes/ne sait pas
OUI	La réponse est oui
NON	La réponse est non
NA	Le contrôle est **sans objet** pour la certification visée

Tableau 2 Options de statut des sous-questions

Préparation à l'examen

Pour obtenir un certificat officiel et devenir un Responsable de la Mise en Œuvre d'Europrivacy, les participants doivent réussir un examen final. Cette section du manuel est destinée à vous préparer et à vous familiariser avec le type d'examen.

L'examen consiste en des questions à choix multiples (50 pour le cours de mise en œuvre) qui doivent être terminées dans le temps imparti (1 heure 15 minutes minutes). Chaque question comporte 4 réponses possibles. Parfois, une seule réponse est correcte, tandis que d'autres fois, il y a plusieurs réponses correctes. Pendant l'examen, un indice vous indiquera si vous devez vous concentrer sur une ou plusieurs bonnes réponses. Pour plus d'informations, vous pouvez vous référer à l'avertissement de l'examen final (Final Exam Disclaimer) sur la page du cours.

L'examen blanc du manuel se compose de 25 questions et il est conseillé de le compléter en 45 minutes. Comme dans l'examen, chaque question comporte 4 réponses possibles. Une réponse correcte à une question vous donne un point. Certaines questions comportent plusieurs réponses correctes et la notation est la suivante :

- 1 point en cas de réponse correcte à une question ;
- 0 point pour l'absence d'une réponse correcte à une question à réponse multiple ;
- 0 point pour une réponse incorrecte, que la ou les bonnes réponses aient été notées ou non.

Pour réussir l'examen blanc, vous devez obtenir 19 points sur 25. Le corrigé est disponible à la fin de la section.

Example

	QUESTION	A	B	C	D
15	Lequel des points suivants n'est PAS un principe clé des certifications Europrivacy ?	Indépendance	Présentation équitable (Fair)	Favoritisme	Confidentialité
16	Parmi les documents suivants, lesquels sont considérés comme des documents normatifs complémentaires d'Europrivacy ?	Lignes directrices Europrivacy pour la réalisation de NOCAR	Règles de communication et de marketing d'Europrivacy	Lignes directrices en matière de responsabilité (accountability) et transparence (openness)	Lignes directrices Europrivacy sur les critères d'utilisation, les vérifications et les contrôles
17	Lequel des éléments suivants fournit des définitions pour le Schéma de Certification Europrivacy ?	Lignes directrices du GDPR et de l'EDPB	Dictionnaire d'Oxford	Autres sources normatives pertinentes, telles que ISO	Wikipédia

Dans ce scénario, l'étudiant a choisi les réponses suivantes (indiquées en orange) :

- Question 15 : C
- Question 16 : D
- Question 17 : A, B et C

La feuille de réponse indique les réponses correctes suivantes :

Numéro de la question	Réponse correcte
15	C
16	B D
17	A C

Cela signifie ce qui suit :

- Si la réponse à la question 15 est correcte, l'élève reçoit un point.
- La réponse à la question 16 est partielle, il manque la réponse B. L'étudiant ne reçoit pas de point.
- Dans la question 17, les réponses A et C sont correctes. Cependant, l'étudiant a également choisi la réponse B qui est incorrecte, ce qui signifie qu'il ne recevra pas de point pour l'ensemble de la question

Explication

Les réponses correctes indiquent la partie des modules à laquelle la question se réfère. En cas d'incertitude, veuillez d'abord étudier attentivement ces points.

Examen blanc

	QUESTION	A	B	C	D
1	Parmi les affirmations suivantes, lesquelles s'appliquent aux Responsables de la Mise en Œuvre ?	Ils travaillent pour des organismes de certification afin de certifier le respect de la protection des données	Ils travaillent pour des cabinets de conseil afin de réduire les risques juridiques et financiers du Propriétaire du Schéma	Ils travaillent pour les organismes de certification afin d'identifier les lacunes potentielles et les non-conformités résiduelles	Ils travaillent pour des cabinets de conseil afin d'aider les candidats avant, pendant et après le processus de certification
2	Laquelle des catégories suivantes peut s'appliquer aux vérifications et aux contrôles ?	E Exemptions	S Spécifique	O Objectif	NC Non conditionnel
3	Parmi les affirmations suivantes, lesquelles sont vraies ?	Toute utilisation de la marque Europrivacy et/ou ECCP nécessite une autorisation écrite et explicite préalable ou une licence de l'Autorité de Protection des Données	Les marques de conformité, les certificats et les déclarations de certification ne doivent pas être utilisés d'une manière susceptible de créer la confusion ou d'induire en erreur quant à la Cible d'Évaluation de la certification visée	L'Organisme de Certification doit exercer un contrôle approprié de la propriété de l'utilisation et de la référence aux certificats qu'il a délivrés	Les traitements de données certifiés peuvent recevoir un certificat Europrivacy, sous le contrôle et l'approbation du Applicant
4	Que se passe-t-il lors d'une réunion de clôture entre le cabinet de conseil et le Applicant ?	Le cabinet de conseil présente une offre complémentaire	Le cabinet de conseil remplit le formulaire de demande à soumettre au Propriétaire du Schéma	Le cabinet de conseil présente les résultats et recueille les commentaires	Le cabinet de conseil présente les auditeurs de l'Organisme de Certification au Applicant
5	Quels sont les critères fondamentaux GDPR Europrivacy ?	Il permet une évaluation systématique de la conformité avec les obligations clés contenues dans le GDPR	Il s'agit d'une liste de contrôle obligatoire que l'Organisme de Certification doit appliquer à chaque traitement de données	Il s'agit d'une liste de contrôle complémentaire à appliquer par l'Autorité Nationale de Protection des Données si le cabinet de conseil en fait la demande	Il permet d'évaluer les exigences en matière de protection des données spécifiques à un domaine ou à une technologie
6	Parmi les affirmations suivantes, lesquelles sont vraies ?	Les organismes de certification ne peuvent pas reproduire les informations publiques figurant sur leur site web	Par défaut, l'Organisme de Certification doit rendre publiques des informations générales sur le processus d'évaluation de la certification	Par défaut, toutes les informations fournies par le Applicant ou relatives au Applicant et à sa certification sont des informations publiques	Les cabinets de conseil sont responsables de la gestion et de la supervision du site Web officiel d'Europrivacy

7	Sous quels formats les critères d'Europrivacy sont-ils disponibles ?	Présentation PowerPoint	Page Sway	Feuilles Excel	Le Propriétaire du Schéma ne met les critères à la disposition de personne
8	Parmi les affirmations suivantes, lesquelles sont vraies ?	L'Autorité de Protection des Données décide du renouvellement d'une certification en fonction des résultats de l'audit de recertification	Au cours des trois années suivant la réception du certificat, le Applicant doit se conformer aux exigences du Schéma de Certification et informer l'Organisme de Certification de tout changement ou problème concernant sa conformité	L'identification d'une non-conformité mineure entraîne automatiquement la suspension et le retrait potentiel de la certification	La certification de référence est basée sur un audit sur site, suivi d'audits de surveillance tous les 5 ans
9	Laquelle des affirmations suivantes s'applique à la colonne "Critères" dans la structure du tableau des critères d'Europrivacy ?	Fournit un identifiant unique et distinct pour chaque vérification et contrôle	Permet à l'équipe d'audit d'identifier certains problèmes ou éléments à traiter par le Applicant	Fournit des indications à l'auditeur sur les sources habituelles d'information	Décrit l'exigence formelle qui doit être mise en œuvre par le Applicant et évaluée par l'auditeur
10	Que doit faire l'Organisme de Certification lorsqu'il reçoit une plainte ou un appel ?	Informer le Applicant de tout problème majeur susceptible de constituer un risque pour le Schéma de Certification ou pour sa réputation	demander à l'Autorité de Protection des Données de prendre toute mesure ultérieure nécessaire pour résoudre la plainte ou l'appel	Recueillir et vérifier toutes les informations pertinentes	Notifier officiellement le résultat de la procédure au plaignant ou au requérant
11	Au cours du processus de préparation à Europrivacy, que doit faire le Responsable de la Mise en Œuvre après avoir signalé les lacunes identifiées ?	Conseiller le client sur la manière de remédier aux lacunes identifiées	Transmettre le rapport au Propriétaire du Schéma	Demander un deuxième avis sur les lacunes à l'Autorité de Protection des Données	Aucune des réponses n'est correcte
12	Parmi les listes de contrôle suivantes, lesquelles sont utilisées dans la phase préliminaire ?	Critères fondamentaux GDPR	Demande et Cible d'Évaluation	Obligations nationales en matière de protection des données	Liste de contrôle de la documentation

13	Qui est tenu de préserver la confidentialité des informations relatives aux certifications ?	Le grand public	Le Propriétaire du Schéma	L'Organisme de Certification	Il ne s'agit pas d'une obligation, mais d'une recommandation
14	Parmi les affirmations suivantes, lesquelles sont vraies ?	Lors de l'évaluation des vérifications et des contrôles d'une section, la Personne Concernée effectue les vérifications et les contrôles demandés	La liste de contrôle des mesures techniques et organisationnelles rassemble les exigences du GDPR applicables à tous les traitements de données	Des vérifications et des contrôles contextuels complémentaires sont spécifiés pour évaluer les exigences en matière de protection des données spécifiques au domaine et à la technologie	Le modèle de liste de non-conformités doit être utilisé par l'Autorité de Protection des Données pour signaler et répertorier les non-conformités identifiées
15	Quelle est la cible principale du Welcome Pack ?	Personnes Concernées	Autorités chargées de la protection des données	Organismes de certification	Applicants
16	Que se passe-t-il si la réglementation applicable en matière de protection des données change pendant la période de maintenance ?	Les changements législatifs n'ont pas d'incidence sur les certifications délivrées	L'Organisme de Certification doit élaborer un plan d'action et le valider avec l'Autorité de Protection des Données	Le Propriétaire du Schéma doit suspendre toutes les certifications délivrées et les invalider	Le Applicant doit évaluer le niveau d'impact sur la validité de la certification
17	Laquelle des affirmations suivantes s'applique à la marque de conformité ?	Il est placé sous le contrôle et l'approbation de l'Organisme de Certification	Il empêche la traçabilité	Il est la propriété du Applicant	Il marque l'accord d'une entreprise sur les décisions d'un Parlement européen
18	Qu'est-ce qui est spécifié dans le mécanisme de plainte et d'appel ?	Qui est chargé du processus au nom de l'EDPB	Qui peut déposer une plainte ou une objection	Une procédure visant à garantir que les mesures correctives appropriées sont prises par l'Autorité de Protection des Données	Les frais supplémentaires qui doivent être payés par le Propriétaire du Schéma à l'Organisme de Certification
19	Parmi les affirmations suivantes, lesquelles sont vraies ?	La Personne Concernée conserve une documentation sur ses tâches et responsabilités concernant ses activités de certification	Le Applicant prend des dispositions contractuelles adéquates pour être informé par le cabinet de conseil certifié	Par défaut, les enregistrements relatifs aux certifications délivrées sont conservés pendant la durée du cycle de certification correspondant, plus 20 ans	L'Autorité Nationale de Protection des Données et le Propriétaire du Schéma peuvent demander l'accès à des informations confidentielles
20	Parmi les éléments suivants, lesquels	Aucune référence incorrecte à la marque de conformité ne figure	Le Applicant a publié une ligne directrice sur l'utilisation des	L'Autorité de Protection des Données est	Que la marque de conformité représente les

	doivent être garantis par l'Organisme de Certification ?	dans la documentation ou dans d'autres publicités	marques de conformité	propriétaire des marques de conformité	convictions des Personnes Concernées à l'égard des processus évalués
21	Parmi les affirmations suivantes, lesquelles sont vraies ?	Les critères Europrivacy et les vérifications et contrôles complémentaires sont applicables et requis pour tous les processus de certification	Le NOCAR est censé évaluer la conformité de la Cible d'Évaluation avec les réglementations du pays dans lequel le Applicant est domicilié	La liste de référence des critères, des vérifications et des contrôles est tenue à jour par les sociétés de conseil agréées par Europrivacy	La liste de contrôle des non-conformités permet de vérifier à l'avance si les politiques et procédures mises en place par le Applicant sont suffisamment complètes pour répondre aux exigences d'Europrivacy
22	Parmi les éléments suivants, lesquels sont inclus dans l'attestation de conformité ?	Le nom et les coordonnées de toutes les personnes certifiées	Les conditions de renouvellement du certificat	Le nom de l'auditeur certifié	Aucune des réponses n'est correcte
23	Parmi les informations suivantes, lesquelles sont disponibles sur le site web d'Europrivacy ?	Le registre en ligne des certificats Europrivacy	Copie des contrats entre les organismes de certification et les Applicants	Bibliothèque en ligne des certifications non retenues	Coordonnées des Applicants certifiés
24	Lequel des points suivants ne s'applique PAS aux activités de surveillance ?	Les activités de surveillance doivent être pleinement soutenues par les Personnes Concernées	Par défaut, une activité de surveillance bimensuelle devrait être la norme	L'Organisme de Certification doit maintenir la certification en démontrant que le Applicant continue à se conformer aux exigences du Schéma de Certification	L'Organisme de Certification sélectionne un ensemble de vérifications et de contrôles à vérifier lors des audits de surveillance
25	Parmi les affirmations suivantes, lesquelles sont vraies ?	Au cours du processus de certification, les cabinets de conseil peuvent aider le Applicant à traiter et à résoudre les éventuelles non-conformités	Pour obtenir une licence, les cabinets de conseil doivent signer un accord écrit avec l'Autorité de Protection des Données avant de fournir tout service lié à l'Europrivacy	Les cabinets de conseil peuvent préparer une offre complémentaire pour fournir un soutien continu au traitement des données certifiées, et pour soutenir la préparation du traitement des données restantes à certifier	Le ECCP aide le Applicant à identifier les deux premières activités de traitement des données à certifier, puis à spécifier formellement la Cible d'Évaluation

Réponses

Numéro de la question	Réponse correcte	Explication
1	D	**Module 1 - Rôle des Responsables de la Mise en Œuvre (diapositive 3)** Les Responsables de la Mise en Œuvre qualifiés travaillent pour des cabinets de conseil et aident les organisations à s'assurer qu'elles respectent en permanence les réglementations applicables en matière de protection des données. Les cabinets de conseil ne se contentent pas de préparer les candidats à la certification de leurs activités de traitement des données, mais les assistent en permanence pendant le processus de certification et la phase de maintenance.
2	A B	**Module 3 - Applicabilité des critères, des vérifications et des contrôles (diapositive 9)** Les critères, les vérifications et les contrôles se répartissent en plusieurs catégories, y compris : obligatoires, exemptions, et spécifiques.
3	B C	**Module 5 - Utilisation des marques de conformité, des licences et des certificats** La question fait référence à plusieurs points du module 5. La *réponse A* est incorrecte car c'est le ECCP, et non l'Autorité de Protection des Données, qui donne son consentement préalable à l'utilisation de la marque Europrivacy. La *réponse D* est incorrecte car les certificats ne sont pas soumis au contrôle et à l'approbation du Applicant mais de l'Organisme de Certification.
4	A C	**Module 1 - Services de post-certification (diapositive 7)** Lors de la réunion de clôture, le cabinet de conseil présente les résultats du processus de préparation, recueille les commentaires du Applicant et, éventuellement, présente une offre complémentaire. La *réponse B* est incorrecte car le formulaire de demande est soumis à l'Organisme de Certification plutôt qu'au Propriétaire du Schéma. La *réponse D* est incorrecte car la présentation des auditeurs ne fait pas partie de la réunion de clôture.
5	A B	**Module 4 - Phase d'évaluation (diapositive 5)** Les critères fondamentaux GDPR constituent la base de tous les processus de certification d'Europrivacy et doivent être appliqués par les auditeurs de l'Organisme de Certification à chaque Cible d'Évaluation, indépendamment de son domaine d'application et de sa localisation. Les critères fondamentaux GDPR permettent une évaluation systématique de la conformité aux obligations clés contenues dans le GDPR.

6	**C**	**Module 2 - Gestion de l'information et confidentialité** Cette question résume les informations du module. En ce qui concerne la *réponse A*, les organismes de certification peuvent reproduire des informations publiques sur leur site web à condition d'obtenir l'approbation du ECCP. *Réponse C* : par défaut, toutes les informations concernant le Applicant doivent être traitées de manière confidentielle. *Réponse D* : il incombe au ECCP, et non aux sociétés de conseil, de tenir à jour le site web d'Europrivacy.
7	**C**	**Module 3 - Critères d'évaluation (diapositive 3)** Les critères, vérifications et contrôles d'Europrivacy sont disponibles dans le Welcome Pack et sur le site web de la communauté Europrivacy sous différentes formes, notamment des fichiers Excel, des fichiers PDF et des modèles Word, afin de faciliter l'évaluation de la conformité.
8	**B**	**Module 5 - Maintenance, renouvellement et appels** Cette question résume les informations du module. *Réponse A*, c'est l'Organisme de Certification et non l'Autorité de Protection des Données qui prend la décision de renouvellement. *Réponse C*, l'identification d'une non-conformité n'entraîne pas automatiquement la suspension ou le retrait de la certification. *Réponse D*, la fréquence des audits de surveillance est fixée à une fois par an, et ils peuvent être effectués sur site ou à distance.
9	**D**	**Module 3 - Structure du tableau (diapositive 12)** Réponses incorrectes : La *réponse A* se réfère à la colonne Ref ID, la *réponse B* se réfère à la colonne Recommandations, tandis que la *réponse C* se réfère à la colonne Mise en œuvre des orientations.
10	**C D**	**Module 6 - Politique d'appels et de plainte (diapositives 8-11)** Réponses incorrectes : *Réponse A* : c'est le Propriétaire du Schéma qui doit être informé. *Réponse B* : l'Autorité de Protection des Données n'est pas responsable de la résolution des plaintes ou des appels.
11	**A**	**Module 1 - Processus de préparation à Europrivacy (diapositives 5)** Les Responsables de la Mise en Œuvre peuvent aider les Applicants à combler les lacunes identifiées. Ils n'ont pas besoin de transmettre ces informations au Propriétaire du Schéma ou de demander un second avis.
12	**B D**	**Module 4 - Phase préliminaire (diapositive 4)** Les critères fondamentaux RGPD (*réponse A*) et les obligations nationales en matière de protection des données (*réponse C*) sont utilisés dans le cadre de la phase d'évaluation.
13	**B C**	**Module 2 - Gestion de l'information et confidentialité**

		La *réponse A* est incorrecte car le grand public n'est pas une partie prenante liée par des règles de confidentialité dans le cadre du processus de certification. De même, la *réponse D* est incorrecte car la confidentialité est une obligation et non une recommandation.
14	**C**	**Module 3 & Module 4** Cette question résume les informations des deux modules sur les critères. La *réponse A* est incorrecte car c'est l'auditeur (et le Responsable de la Mise en Œuvre), et non la Personne Concernée, qui effectue les vérifications et les contrôles. La *réponse B* est incorrecte, car ce sont les critères fondamentaux GDPR, et non la liste de contrôle TOM, qui rassemblent les exigences GDPR. La *réponse D* est incorrecte, car c'est l'auditeur (et le Responsable de la Mise en Œuvre) qui peut utiliser la liste des non-conformités pour établir un rapport sur les non-conformités.
15	**D**	**Module 1 - Rôle des Responsables de la Mise en Œuvre (diapositive 3)** Les cabinets de conseil peuvent s'appuyer sur l'offre Europrivacy Welcome Pack pour apporter un soutien complet à leurs Applicants.
16	**D**	**Module 6 - Changements affectant la certification (diapositive 6)** Les modifications apportées à la réglementation applicable en matière de protection des données, telles que les révisions législatives, les décisions des tribunaux nationaux ou supranationaux, les décisions de l'EDPB ou les décisions de la Commission européenne, sont suivies et traitées par l'Organisme de Certification. Si ces changements ont un impact sur les certifications délivrées, l'Organisme de Certification : (1) évalue le niveau d'impact sur la validité de la certification ; (2) élabore un plan d'action ; (3) contacte l'Autorité de Protection des Données concernée et demande la validation du plan d'action proposé ; (4) met en œuvre le plan d'action une fois qu'il a été approuvé par l'Autorité de Protection des Données.
17	**A**	**Module 5 - Marque de conformité (diapositive 9)** Les activités de traitement des données certifiées peuvent porter la marque de conformité Europrivacy, sous le contrôle et l'approbation de l'Organisme de Certification.
18	**B**	**Module 6 - Politique en matière d'appels et de plaintes (diapositive 9)** La *réponse A* est incorrecte car elle est donnée au nom de l'Organisme de Certification et non de l'EDPB. La *réponse C* est incorrecte car ce n'est pas l'Autorité de Protection des Données mais l'Organisme de Certification ou le Propriétaire du Schéma.

		La *réponse D* est incorrecte car il n'y a pas de frais supplémentaires à payer au Propriétaire du Schéma.
19	**D**	**Module 2 - Gestion de l'information et confidentialité** Cette question résume les informations du module. La *réponse A* est incorrecte car ce n'est pas à la Personne Concernée mais à l'Organisme de Certification qu'il incombe de tenir des registres sur les activités de certification. La *réponse B* est incorrecte car c'est l'Organisme de Certification qui établit les accords contractuels avec les Applicants certifiés. La *réponse C* est incorrecte car les enregistrements sont conservés pendant 10 ans.
20	**A**	**Module 5 - Contrôle de l'Organisme de Certification (diapositive 13)** La *réponse B* est incorrecte car c'est le Propriétaire du Schéma qui a publié des lignes directrices sur l'utilisation des marques de conformité. De même, la *réponse C* est incorrecte car c'est l'Organisme de Certification qui exerce le contrôle de la propriété sur les marques de conformité. La *réponse D* est incorrecte car les marques de conformité sont un sceau ou une marque qui peut être utilisée pour indiquer que la procédure de certification a été menée à bien.
21	**A B**	**Module 3 & Module 4** Cette question résume les informations des deux modules sur les critères. La *réponse C* est incorrecte car c'est le Propriétaire du Schéma et non un cabinet de conseil qui tient à jour la liste de référence. La *réponse D* est incorrecte, car la liste de contrôle de la liste des non-conformités sert à signaler et à énumérer les non-conformités identifiées que le Applicant doit corriger pour être certifié.
22	**D**	**Module 5 - Déclarations de conformité (diapositive 10)** Aucune de ces réponses n'est correcte car la déclaration de conformité comprend : la référence à Europrivacy et, lorsqu'il est autorisé, le logo Europrivacy ; le nom du Applicant certifié ; le cas échéant, le nom du ou des contrôleurs conjoints ; une indication claire de la Cible d'Évaluation et de sa portée géographique ; le cas échéant, une indication claire des normes ou exigences complémentaires qui ont été ajoutées ;les dates de délivrance et de validité du certificat ; l'identifiant unique du certificat délivré ; la mention "Informations détaillées à" suivie du nom de domaine du site web du schéma de certification et du registre en ligne des certificats ; et le nom et l'adresse de l'Organisme de Certification qui délivre le certificat.
23	**A**	**Module 2 - Gestion de l'information et confidentialité** Le registre en ligne des certificats Europrivacy est disponible sur le site web d'Europrivacy.

24	**A B**	**Module 6 - Audits de suivi et de surveillance (diapositive 5)** La *réponse A* ne s'applique pas aux audits de surveillance car les Personnes Concernées n'ont pas besoin de soutenir ces activités. La *réponse B* ne s'applique pas aux audits de surveillance, car les activités ont lieu tous les ans et non tous les deux mois.
25	**A C**	**Module 1 - Rôle des Responsables de la Mise en Œuvre** Cette question résume les informations du module. La *réponse B* est incorrecte car les cabinets de conseil doivent signer un accord avec le ECCP et non avec l'Autorité de Protection des Données pour fournir des services liés à Europrivacy. La *réponse D* est incorrecte car c'est le cabinet de conseil, et non le ECCP, qui aide le Applicant à sélectionner les deux premières activités de traitement des données.