SUPPORT & CAS CORRIGÉS · 13 SEPTEMBRE 2026

RGPD : protéger les données et piloter la conformité

Support pédagogique Beyond Expertise. Validation du formateur à réaliser avant animation ; aucune certification officielle revendiquée.

Mode d’emploi

Deux journées de 7 heures hors pauses, avec ateliers et échanges. Chaque séquence dure 105 minutes ; la dernière inclut le quiz de 20 minutes. La durée ne correspond pas au seul temps de lecture des pages. Les approfondissements sont sélectionnés avec le formateur selon le positionnement et le temps disponible.

Lecture commentée, huit ateliers sur cas fictifs, correction guidée, dossier de synthèse et quiz formatif de 20 questions. Les supports sont consultables en local ; le formateur doit valider et adapter l’animation.

Positionnement

- Quel traitement suivez-vous dans votre activité ?
- Distinguez-vous consentement et contrat ? Donnez un exemple.
- Qui peut accéder aujourd’hui à vos données de formation ?
- Quelle décision souhaitez-vous savoir prendre à la fin du parcours ?

Cas fil rouge

Le centre fictif Horizon Compétences prépare des formations pour 120 salariés. Il utilise un CRM, un LMS et un outil de visioconférence. Un fichier de suivi contient des emails, des notes et un commentaire médical. Vous auditez la chaîne puis gérez un envoi à un mauvais destinataire.

Séquence 1 · Reconnaître un traitement et répartir les responsabilités

RGPD : articles 2 à 5, 24, 26 et 28

Une donnée personnelle concerne une personne physique identifiable, même si son nom est absent. Un identifiant de salarié, un email professionnel nominatif ou une combinaison rare de poste et de site peuvent permettre une identification. Remplacer le nom par un numéro constitue généralement une pseudonymisation : si une correspondance ou un recoupement demeure possible, le RGPD continue de s’appliquer.

Un traitement est une opération ou un ensemble d’opérations sur ces données : collecter, consulter, exporter, corriger et supprimer en font partie. Commencez par décrire le résultat recherché, puis les personnes, données, destinataires et outils nécessaires. « Gérer toutes nos données » est trop vague. « Organiser les inscriptions et suivre la participation à une session » permet déjà de questionner chaque champ.

Le responsable de traitement décide pourquoi les données sont utilisées et des moyens essentiels. Un prestataire qui traite uniquement pour son compte et selon ses instructions est un sous-traitant. Le nom donné dans le contrat ne suffit pas : regardez les décisions réelles. Deux acteurs qui définissent ensemble les finalités et moyens peuvent être responsables conjoints. Un fournisseur peut aussi agir comme responsable distinct pour un usage propre ; cet usage doit être examiné séparément.

Appliquez les principes de l'article 5 comme des questions de conception : l'usage est-il loyal et expliqué ? Les champs sont-ils nécessaires ? Les données sont-elles exactes ? Quand doivent-elles être supprimées ou archivées ? Qui les protège ? Quelle pièce permet de démontrer la décision ? Une politique écrite sans pratique correspondante ne répond pas à la dernière question.

Dans un centre de formation, l'employeur commanditaire, le centre et l'hébergeur du LMS n'ont pas automatiquement le même rôle. Le centre peut décider de ses obligations de suivi ; l'hébergeur peut agir sur ses instructions. Documentez le partage réel des responsabilités avant tout échange.

Mise en pratique

Horizon conserve : nom, email professionnel, identifiant salarié, résultat au quiz, numéro de sécurité sociale et diagnostic médical. Le LMS stocke ces champs sur instruction du centre. Classez les données, proposez deux suppressions et décrivez les rôles du centre, de l'employeur et du LMS. Ne supposez pas que l'employeur a besoin du détail de chaque réponse au quiz.

Corrigé pédagogique

Nom, email, identifiant et score sont des données personnelles. Le diagnostic est une donnée de santé ; le numéro de sécurité sociale relève aussi de règles spécifiques. Leur présence dans un suivi pédagogique courant n'est pas justifiée par le seul intérêt du centre : les retirer de ce fichier, puis traiter séparément un éventuel besoin légal ou d'aménagement avec accès limité. Le rôle du LMS décrit correspond à une sous-traitance. Le centre et l'employeur doivent qualifier leurs usages respectifs ; le seul financement ne rend pas l'employeur responsable de tous les traitements. Livrable attendu : une ligne par finalité et acteur, sans qualifier les fichiers pseudonymisés d'anonymes.

Séquence 2 · Choisir une base légale et limiter la collecte

RGPD : articles 5, 6, 7, 9 et 25

La base légale se choisit pour une finalité avant de collecter. Le RGPD prévoit le consentement, le contrat ou les mesures précontractuelles demandées par la personne, l'obligation légale, la sauvegarde des intérêts vitaux, la mission d'intérêt public et l'intérêt légitime. Il ne s'agit pas de six cases interchangeables : la situation doit satisfaire les conditions de la base retenue.

Le contrat couvre ce qui est objectivement nécessaire au service demandé par la personne concernée. Un contrat signé entre deux entreprises ne suffit pas à justifier automatiquement tous les usages des données de leurs salariés. Pour une obligation légale, identifiez le texte et les données qu'il impose réellement. Pour l'intérêt légitime, documentez l'objectif, la nécessité et la balance avec les droits et attentes raisonnables des personnes ; prévoyez l'opposition lorsqu'elle s'applique.

Le consentement suppose un choix libre, éclairé, spécifique et un acte positif. Une case précochée ou la simple poursuite de la navigation ne convient pas. Pouvoir retirer son choix aussi facilement qu'on l'a donné est essentiel. Évitez une case unique mélangeant traitement nécessaire de la demande, publicité et publication d'une photo. La notice d'information explique ; elle n'est pas, par elle-même, une demande de consentement.

Les données de santé et autres catégories de l'article 9 demandent, en plus d'une base de l'article 6, une exception pertinente à leur interdiction de principe. Le consentement explicite n'est pas une solution automatique, notamment lorsque le choix ne peut être libre. Pour un aménagement, demandez d'abord le besoin pratique, sans diagnostic dans un formulaire public.

La protection dès la conception consiste à réduire le problème avant de le sécuriser : champ facultatif, période courte, accès restreint, données fictives pour les tests. Chaque champ devrait avoir une phrase de justification. « Cela pourrait servir plus tard » ne suffit pas.

Mise en pratique

Réécrivez un formulaire d'information demandant nom, email, adresse personnelle, date de naissance, handicap et accord obligatoire à la newsletter. Il sert seulement à recevoir le programme RGPD. Distinguez champs nécessaires, facultatifs et à supprimer ; proposez une base pour la réponse et une règle distincte pour la prospection.

Corrigé pédagogique

Un moyen de réponse et le programme demandé sont nécessaires ; le nom peut être limité au besoin réel de personnalisation. Adresse personnelle, naissance et diagnostic sont inutiles à cet objectif. Retirer l'abonnement obligatoire. Selon la situation, la réponse peut relever de mesures précontractuelles demandées ou d'un intérêt légitime documenté. La prospection doit faire l'objet de son analyse propre, y compris les règles françaises de prospection électronique ; ne pas déduire un accord marketing de la demande du programme. Fournir une courte information avec un lien vers la notice complète.

Séquence 3 · Informer et répondre aux demandes de droits

RGPD : articles 12 à 22 et 77

Une information utile répond aux questions du visiteur : qui utilise mes données, pourquoi, sur quelle base, avec qui, pendant combien de temps et comment exercer mes droits ? Les articles 13 et 14 distinguent la collecte auprès de la personne et celle provenant d'un tiers. Le bon moment et certaines mentions diffèrent ; un lien discret ajouté longtemps après la collecte ne règle pas le problème.

La notice identifie le responsable, les contacts utiles et le DPO s'il existe. Elle précise finalités, bases légales, intérêts légitimes éventuels, destinataires, conservation ou critères, transferts éventuels et garanties, droits, plainte auprès de l'autorité, caractère obligatoire des données et conséquences d'un refus. Une décision automatisée relevant de l'article 22 appelle des informations spécifiques. Présentez une première couche près du formulaire puis le détail accessible.

À réception d'une demande, consignez la date, le périmètre et le canal de réponse. Le délai de principe est un mois. Une prolongation pouvant aller jusqu'à deux mois supplémentaires est possible selon la complexité et le nombre de demandes ; informez-en la personne, avec les raisons, dans le premier mois. Ne retardez pas artificiellement l'enregistrement en demandant une pièce d'identité systématique. En cas de doute raisonnable, demandez seulement les éléments nécessaires à la vérification.

Les droits ne sont pas tous absolus. Une demande d'effacement peut se heurter à une conservation légalement nécessaire. Expliquez alors les catégories maintenues, le motif et les voies de recours. L'accès inclut une copie des données concernées ; protégez les données de tiers sans refuser l'ensemble par facilité. La portabilité a un champ particulier : traitement automatisé fondé sur le consentement ou le contrat, pour les données fournies par la personne.

Traitez aussi les conséquences opérationnelles : correction dans les exports actifs, information des destinataires lorsque requise, suppression planifiée dans les sauvegardes et prévention d'une réapparition lors d'une restauration. Gardez une trace proportionnée de la réponse, sans créer un dossier d'identité excessif.

Mise en pratique

Le 31 janvier, une ancienne participante demande ses résultats, la rectification de son nom et l'effacement de toutes ses données. Le registre comprend aussi des commentaires concernant d'autres personnes. Rédigez un plan de traitement et une réponse d'accusé de réception ; distinguez accès, rectification et effacement.

Corrigé pédagogique

Enregistrer trois demandes liées et fixer l'échéance au dernier jour du mois suivant lorsque le jour correspondant n'existe pas. Vérifier l'identité de façon proportionnée au risque avant de communiquer des résultats. Préparer une copie des données de la participante, en occultant ce qui porte atteinte aux tiers. Corriger le nom après vérification. Identifier les éventuelles obligations de conservation avant de promettre l'effacement total. L'accusé confirme le périmètre et la date prévue ; il ne dit ni « tout est supprimé » ni « une pièce d'identité est toujours obligatoire ». Documenter une éventuelle prolongation avant l'échéance.

Séquence 4 · Tenir le registre et maîtriser les prestataires

RGPD : articles 28, 30, 32 et 44 à 49

Le registre décrit des activités, pas simplement une liste de logiciels. Une même application peut servir l'inscription, l'évaluation et la prospection : les finalités, destinataires et conservations diffèrent. Pour chaque activité, indiquez le responsable et les contacts, les finalités, les catégories de personnes et de données, les destinataires, les transferts, les délais envisagés d'effacement et une description générale des mesures de sécurité. Ajoutez une base légale, un pilote et une date de revue pour faciliter le suivi.

L'exception au registre pour certaines organisations de moins de 250 personnes est limitée. Un traitement non occasionnel ou présentant un risque, ou portant sur certaines catégories de données, peut écarter cette exception. Un centre utilisant chaque semaine un LMS ne devrait donc pas conclure « petite structure, pas de registre » sans analyse.

Avant de confier des données à un fournisseur, vérifiez ses garanties et contractualisez les instructions. L'article 28 couvre notamment confidentialité, sécurité, assistance pour les droits et les incidents, sous-traitants ultérieurs, fin de contrat et possibilité de démonstration ou d'audit. Demandez des éléments exploitables : politique de sauvegarde, réversibilité testable, délai de remontée d'incident, liste des sous-traitants et lieux d'accès.

« Hébergé en Europe » ne répond pas à toutes les questions. Un support technique situé hors de l'Espace économique européen peut accéder aux données. Qualifiez le flux et le mécanisme applicable : décision d'adéquation dans son périmètre, garanties appropriées comme des clauses contractuelles types avec l'analyse nécessaire, ou dérogation dans des conditions limitées. Une clause signée ne dispense pas d'évaluer le contexte réel.

À la sortie du fournisseur, organisez l'export utile, la révocation des accès et la suppression ou restitution prévue. Conservez la preuve de ces opérations. Réévaluez les changements de sous-traitants et de finalités, plutôt que de classer définitivement le contrat après signature.

Mise en pratique

Le fournisseur LMS propose un hébergement à Paris, un support hors EEE et un usage des réponses des apprenants pour améliorer son propre produit. Sa clause indique seulement « service conforme RGPD ». Rédigez cinq questions bloquantes et complétez une fiche de registre de l'activité d'évaluation.

Corrigé pédagogique

Demander les instructions et rôles précis pour chaque usage, le contrat article 28 complet, les lieux et personnes ayant accès, les sous-traitants ultérieurs et mécanismes de transfert, puis les modalités de restitution et suppression. L'amélioration pour compte propre doit être qualifiée séparément ; elle ne devient pas licite parce que la clause la mentionne. La fiche d'évaluation décrit apprenants, identifiants et résultats, accès formateur attribué, conservation à justifier et mesures de restriction. Ne pas inscrire « aucun transfert » tant que l'accès support n'est pas analysé.

Séquence 5 · Sécuriser, conserver et décider d’une AIPD

RGPD : articles 5, 25, 32, 35 et 36

La sécurité ne se réduit pas au mot de passe. Identifiez ce qui arriverait aux personnes si les données étaient divulguées, modifiées ou perdues : discrimination, préjudice financier, perte d’accès à une formation ou exposition d’une situation médicale. Évaluez vraisemblance et gravité, puis choisissez les mesures en fonction de ce risque.

Commencez par des contrôles vérifiables : compte individuel, droits limités aux groupes attribués, révocation au départ, authentification renforcée pour les accès sensibles, mises à jour, chiffrement approprié, sauvegardes protégées et restauration testée. Un fichier exporté échappe souvent aux permissions du LMS : limitez ses destinataires, sa durée de présence et son emplacement. Un journal d’audit doit aider à enquêter sans enregistrer inutilement mots de passe, messages privés ou copies complètes de formulaires.

Il n’existe pas une durée RGPD universelle pour toutes les données. Distinguez la base active, l’archivage intermédiaire justifié et la suppression. Pour chaque catégorie, définissez le déclencheur, la durée, le motif légal ou opérationnel et les personnes ayant accès. Les sauvegardes ont un cycle propre ; une restauration doit réappliquer les suppressions nécessaires. Testez d’abord la liste des éléments concernés avant toute purge.

Une analyse d’impact relative à la protection des données (AIPD) est requise lorsqu’un traitement est susceptible d’engendrer un risque élevé pour les droits et libertés. Examinez l’article 35, les listes de l’autorité et les critères pertinents, notamment données sensibles, personnes vulnérables, surveillance et évaluation systématique. Une nouvelle technologie est un signal d’analyse, pas la preuve automatique qu’une AIPD suffit ou qu’elle est toujours obligatoire.

L’AIPD décrit le traitement, sa nécessité et sa proportionnalité, les risques et les mesures. Faites-la avant le lancement et revoyez-la lorsque le risque change. Si le risque élevé subsiste malgré les mesures envisagées, l’article 36 prévoit une consultation préalable de l’autorité. Le responsable conserve la décision ; le DPO, s’il existe, conseille sans devenir seul responsable de la conformité.

Mise en pratique

Un centre veut croiser absences, scores et besoins d’aménagement pour prédire les abandons. Tous les formateurs pourraient voir tous les profils. Proposez des mesures immédiates et les questions permettant de décider d’une AIPD. Définissez une règle de conservation à soumettre au responsable, sans inventer un délai réglementaire.

Corrigé pédagogique

Suspendre la collecte des détails médicaux inutiles et limiter les accès aux personnes habilitées. Clarifier l’objectif, le lien entre données et résultat, les personnes concernées et les effets d’un classement erroné. Examiner évaluation/profilage, vulnérabilité possible et santé, puis documenter le besoin d’AIPD selon les critères applicables. Prévoir une alternative moins intrusive et un contrôle humain. Une proposition de conservation doit préciser catégories, déclencheur, durée envisagée et justificatif à valider ; « cinq ans parce que c’est le RGPD » n’est pas une justification.

Séquence 6 · Réagir à une violation de données

RGPD : articles 4(12), 28, 33 et 34

Une violation peut être un mauvais destinataire, un compte compromis, une suppression accidentelle ou une indisponibilité de données personnelles. La première action est de contenir l’incident sans détruire les preuves : retirer un lien exposé, suspendre un compte ou isoler un poste, puis conserver une chronologie factuelle. Ne promettez pas qu’un email a été effacé chez un tiers sans vérification.

Le responsable analyse les catégories et le volume de données, les personnes concernées, l'identifiabilité, les protections, la durée d'exposition et les conséquences possibles. Un fichier chiffré dont la clé est réellement protégée ne se traite pas comme une liste médicale ouverte. Documentez aussi les inconnues et la façon de les lever.

La notification à l'autorité est requise sauf si la violation n'est pas susceptible d'engendrer un risque pour les droits et libertés. Lorsqu'elle est requise, elle intervient dans les meilleurs délais et, si possible, au plus tard 72 heures après en avoir pris connaissance. Un retard doit être motivé ; l'information peut être complétée progressivement lorsque tous les éléments ne sont pas disponibles. Le sous-traitant alerte le responsable sans délai indu, au lieu d'attendre sa propre échéance de 72 heures.

En cas de risque élevé, informer aussi les personnes sans délai indu, sous réserve des conditions et exceptions applicables. Cette communication doit permettre d'agir : nature de l'incident, contact, conséquences et mesures. Elle ne se résume pas à une formule rassurante. Évitez de republier les données exposées dans le message d'alerte.

Toutes les violations doivent être documentées, y compris celles non notifiées. Le journal conserve les faits, effets et mesures prises ; la justification de la décision permet sa réévaluation si de nouveaux faits apparaissent. Terminez par une correction testée : restriction d'export, contrôle du destinataire, formation ciblée ou alerte sur les liens publics.

Mise en pratique

Vendredi à 16 h, Horizon découvre qu'un fichier de 120 participants, comprenant 12 commentaires médicaux, a été envoyé à une entreprise cliente non concernée. Le destinataire affirme l'avoir supprimé, sans preuve. Produisez la chronologie des deux premières heures, une analyse du risque et les éléments d'une notification éventuelle.

Corrigé pédagogique

Consigner découverte et faits connus, bloquer les autres accès, solliciter la suppression et préserver les éléments d'enquête. Alerter le responsable et le référent compétent. Les données de santé et le destinataire externe rendent un risque plausible ; ne pas classer l'affaire sans examen. Préparer la notification à l'autorité compétente si les conditions sont remplies, sans attendre le lundi ; 72 heures après vendredi 16 h correspond à lundi 16 h, mais l'obligation reste d'agir au plus tôt. Évaluer séparément le risque élevé et l'information des personnes. Documenter les inconnues, le nombre approximatif de personnes et d'enregistrements, les conséquences, mesures et contact.

Séquence 7 · Cookies, marketing et données dans les outils d'IA

RGPD : articles 5 à 7, 13, 21, 25 et 28 ; article 82 de la loi Informatique et Libertés

Un cookie de session exclusivement nécessaire à la connexion demandée peut être exempté de consentement. Un traceur publicitaire ne le devient pas parce qu'il porte le même nom ou se trouve sur la même page. Le raisonnement vise aussi des techniques comme certains stockages locaux, pixels ou empreintes, pas seulement les fichiers appelés cookies.

Faites un inventaire des requêtes et stockages avant d'ajouter une bannière. Déclenchez les usages soumis au consentement uniquement après le choix ; rendez le refus aussi simple que l'acceptation et le retrait facile à retrouver. Ne bloquez pas l'accès au contenu principal pour obtenir l'accord à une vidéo décorative facultative. Lorsque le site n'a aucun usage soumis au consentement, un bandeau « tout accepter » peut induire en erreur : une information exacte suffit pour les opérations exemptées.

Une connexion à un fournisseur externe peut communiquer l'adresse IP et des informations techniques même sans cookie. Documentez finalité, destinataire et transferts éventuels ; héberger un élément soi-même ou le remplacer par un rendu local peut supprimer ce flux. Le bouton de refus n'efface pas les données déjà

transmises avant son affichage.

Une demande de devis ne vaut pas abonnement marketing. Séparez la réponse attendue et la prospection ; examinez les règles françaises applicables au destinataire et au canal, en plus du RGPD. Pour la prospection directe, l'opposition doit être effectivement prise en compte. Conserver une liste minimale d'opposition peut éviter de réimporter une personne exclue.

Un prompt envoyé à un service d'IA peut contenir des données personnelles ou des secrets. L'absence d'entraînement annoncée n'implique pas l'absence de stockage, d'accès support ou de sous-traitants. Vérifiez les conditions, réglages et contrats. Utilisez des exemples fictifs ou expurgés, sans considérer automatiquement qu'un simple retrait du nom rend le dossier anonyme.

Mise en pratique

La page d'accueil charge une vidéo externe, une mesure publicitaire et un cookie de connexion. L'équipe colle également des demandes de handicap dans un assistant d'IA gratuit. Proposez un ordre de correction, puis rédigez une phrase marketing exacte après suppression des deux chargements facultatifs.

Corrigé pédagogique

Stopper l'envoi de données médicales au service non autorisé et traiter les envois antérieurs comme un sujet à investiguer. Bloquer les traceurs publicitaires avant consentement, ou les supprimer si inutiles ; supprimer ou rendre facultatif le flux vidéo. Garder le cookie strictement nécessaire avec information claire. Exemple après vérification : « L'accueil fonctionne sans vidéo externe ni traceur publicitaire. » Éviter « vos données ne quittent jamais votre appareil » si des formulaires et ressources pédagogiques utilisent encore un serveur ou un fournisseur.

Séquence 8 · Soutenir un dossier de conformité et prioriser les actions

RGPD : articles 5(2), 24, 30, 37 à 39 et 42 ; synthèse du parcours

Une conformité démontrable relie une exigence, une pratique et une preuve datée. Une fiche de registre dit ce qui doit se passer ; un contrôle des droits d'accès montre ce qui se passe. Un modèle vierge n'est pas une preuve d'exécution et un test sur données fictives ne prouve pas le traitement correct d'un incident réel. Classez explicitement ces trois niveaux.

Le DPO n'est pas obligatoire pour toute PME. Examinez les conditions de l'article 37, notamment organisme public dans son périmètre, suivi régulier et systématique à grande échelle ou traitements à grande échelle de catégories particulières de données dans les activités de base. Lorsqu'un DPO est désigné, assurez ressources, indépendance, absence de conflit d'intérêts et accès à la direction. Une certification de compétences peut être utile mais n'est pas une condition universelle pour exercer. La responsabilité de l'organisme demeure.

Le RGPD est un règlement. Une certification volontaire peut porter sur un périmètre précis de traitement ou sur un processus de formation ; elle n'autorise pas à déclarer tous les traitements conformes. Une attestation délivrée à la fin de ce parcours constate une formation et, si elles sont réalisées, les évaluations. Elle n'est ni une certification DPO, ni un titre RNCP/RS, ni une approbation de la CNIL.

Priorisez les corrections par conséquences pour les personnes et capacité d'action. Une exposition publique de données de santé passe avant une amélioration de mise en page. Attribuez à chaque action un responsable, une échéance, une preuve attendue et une vérification d'efficacité. Utilisez des statuts compréhensibles : à instruire, en cours, vérifié, avec réserve motivée.

Pour la soutenance, présentez vos choix et leurs limites. Dire « la base légale reste à confirmer car le contrat ne couvre pas cet usage » est plus utile qu'une case verte sans justification. Le formateur évalue le raisonnement

et les livrables ; la réussite d'un quiz seul ne certifie pas l'organisme de l'apprenant.

Mise en pratique

Dossier final Horizon : rendre une fiche de registre, une notice, une réponse de droits, une fiche d'incident et cinq actions classées par priorité. En 10 minutes, défendre deux décisions contestables devant le groupe. Terminer le quiz individuel en 20 minutes. Les 30 dernières minutes servent à la correction et au plan de transfert dans son activité.

Corrigé pédagogique

Barème proposé : qualification et minimisation 20 points ; bases légales et information 20 ; droits et conservation 20 ; sécurité, fournisseur et incident 25 ; priorisation avec preuves 15. Seuil pédagogique proposé : 70/100 au dossier et 70 % au quiz, avec reprise des points insuffisants. Une fuite ignorée, une fausse certification ou une absence de vérification d'identité avant divulgation appelle une reprise même si le total est atteint. Le formateur consigne son appréciation réelle ; aucune soutenance ni compétence n'est validée automatiquement par la simple lecture.

Quiz formatif et corrigé

1. Un fichier remplace les noms par des identifiants reliés à une table séparée. Il est…

- 1. pseudonymisé et reste généralement soumis au RGPD
- 2. anonyme dans tous les cas
- 3. hors RGPD si la table est chiffrée

Réponse 1. La possibilité de réidentifier maintient le caractère personnel ; la pseudonymisation est une mesure de réduction du risque, pas une sortie automatique du RGPD.

2. Qui décide de la finalité et des moyens essentiels ?

- 1. toujours le DPO
- 2. le responsable de traitement
- 3. toujours l'hébergeur

Réponse 2. La qualification repose sur les décisions réelles. Le prestataire informatique peut être sous-traitant, et le DPO conseille.

3. Pour une demande de programme, faut-il imposer l'accord à la newsletter ?

- 1. Oui, car le programme est gratuit
- 2. Oui, si une notice existe
- 3. Non, il faut distinguer les deux finalités

Réponse 3. Un service demandé ne doit pas imposer une prospection distincte. Le choix de la base et les règles de prospection doivent être examinés séparément.

4. Une base légale doit être…

- 1. justifiée pour la finalité avant la collecte
- 2. choisie après une plainte
- 3. toujours le consentement

Réponse 1. Les bases de l’article 6 ont des conditions propres ; il faut définir l’usage et sa justification avant de recueillir les données.

5. Un besoin d’aménagement impose-t-il de collecter un diagnostic dans le formulaire public ?

- 1. Oui, si l’accès administrateur est protégé
- 2. Non, demander d’abord le besoin pratique nécessaire
- 3. Oui, pour tout participant

Réponse 2. La sécurité ne rend pas une collecte excessive nécessaire. Les données de santé demandent un examen spécifique.

6. Le délai de principe pour répondre à une demande de droits est…

- 1. 72 heures
- 2. six mois
- 3. un mois

Réponse 3. L’article 12 prévoit un mois ; la prolongation éventuelle doit être justifiée et annoncée dans ce délai initial.

7. Peut-on demander systématiquement une copie de pièce d’identité ?

- 1. Non, la vérification doit être proportionnée au doute et au risque
- 2. Oui, même pour corriger une coquille
- 3. Non, aucune vérification n’est jamais permise

Réponse 1. Il faut éviter de divulguer à un imposteur sans créer une collecte systématique excessive. Des éléments supplémentaires sont possibles en cas de doute raisonnable.

8. Une demande d’effacement implique…

- 1. de la refuser si la personne a suivi une formation
- 2. d’examiner les données, les motifs de conservation et les exceptions
- 3. de supprimer immédiatement toutes les archives légales

Réponse 2. L’effacement n’est ni absolu ni exclu par principe. La réponse doit expliquer les données supprimées et les éventuelles catégories conservées.

9. Une PME utilise chaque semaine un LMS. L’exemption de registre…

- 1. est automatique pour toute PME
- 2. dépend seulement du prix du logiciel
- 3. ne se déduit pas du seul effectif inférieur à 250

Réponse 3. Le caractère non occasionnel et les autres conditions de l’article 30 doivent être examinés.

10. Une clause « conforme RGPD » dans un contrat fournisseur…

- 1. ne remplace pas les clauses et garanties requises
- 2. suffit à démontrer toute conformité
- 3. transfère toute responsabilité au fournisseur

Réponse 1. Instructions, sécurité, assistance, sous-traitance ultérieure et fin de contrat doivent être traitées selon les rôles réels.

11. Un serveur en France avec un support hors EEE…

- 1. rend le RGPD inapplicable au support
- 2. demande l'analyse des accès et des transferts éventuels
- 3. exclut nécessairement tout transfert

Réponse 2. La localisation du serveur ne décrit pas tous les flux ni tous les accès.

12. Une durée de conservation doit être…

- 1. toujours fixée à cinq ans
- 2. illimitée tant que le stockage est chiffré
- 3. justifiée par catégorie, finalité et déclencheur

Réponse 3. La limitation de conservation s'applique même aux données protégées. Les obligations légales doivent être identifiées.

13. Une AIPD est à examiner notamment quand…

- 1. le traitement est susceptible de créer un risque élevé pour les personnes
- 2. le logiciel coûte plus de 1 000 euros
- 3. un fichier possède plus de dix colonnes

Réponse 1. L'analyse repose sur les droits et libertés, les critères et listes applicables ; le prix n'est pas un critère.

14. Une violation sans risque susceptible pour les personnes…

- 1. doit toujours être publiée sur le site
- 2. reste à documenter même si elle n'est pas notifiée
- 3. doit être oubliée immédiatement

Réponse 2. Le registre des violations permet de démontrer l'analyse et de réévaluer la décision si les faits changent.

15. Quand une notification à l'autorité est requise, le délai visé est…

- 1. 72 heures après la fin de l'enquête dans tous les cas
- 2. un mois après le dépôt d'une plainte
- 3. au plus tôt et si possible sous 72 heures après connaissance

Réponse 3. Ne pas attendre l'enquête complète : les informations peuvent être complétées progressivement. Un retard se justifie.

16. Informer aussi les personnes après une violation dépend notamment…

- 1. d'un risque élevé, avec les conditions et exceptions applicables
- 2. de l'existence d'un abonnement marketing
- 3. du seul nombre de fichiers concernés

Réponse 1. L'article 34 vise le risque élevé. L'information doit donner les conséquences et mesures utiles.

17. Un cookie exclusivement nécessaire à la session demandée…

- 1. autorise le suivi publicitaire dans le même cookie
- 2. peut être exempté de consentement avec information adaptée
- 3. exige forcément une bannière publicitaire

Réponse 2. L'exemption vise une finalité strictement nécessaire ; elle ne couvre pas les finalités additionnelles.

18. Copier un dossier médical sans nom dans un assistant public…

- 1. est toujours anonyme
- 2. est licite dès que le service promet de ne pas entraîner son modèle
- 3. peut encore exposer des données personnelles identifiables

Réponse 3. Les recoupements, la base légale, les conditions du fournisseur et les données sensibles restent à examiner.

19. Le DPO est-il obligatoire pour toute entreprise ?

- 1. Non, les conditions de désignation doivent être examinées
- 2. Oui, même sans traitement de données
- 3. Non, seules les banques peuvent en désigner

Réponse 1. L'article 37 décrit les situations obligatoires. Une désignation volontaire est également possible avec les garanties correspondantes.

20. La réussite de cette formation…

- 1. vaut agrément de la CNIL
- 2. ne certifie ni l'entreprise ni les compétences DPO au titre d'un mécanisme officiel
- 3. rend automatiquement tous les traitements conformes

Réponse 2. Une attestation de formation doit rester fidèle à son objet. Les certifications volontaires ont un périmètre et une procédure propres.

Sources

- RGPD — règlement (UE) 2016/679, texte officiel
- CNIL — certifications volontaires des formations et des compétences
- CNIL — règles relatives aux cookies et traceurs
- CNIL — violations de données : les règles à suivre
- CNIL — recueillir le consentement des personnes