Incidents et notification.

Version 1.0 · en vigueur le 15 novembre 2026

1. Objet et portée

1.1. Ce qu'est un incident. Un incident de sécurité est un événement qui porte atteinte, ou menace de porter atteinte, à la confidentialité, à l'intégrité ou à la disponibilité d'informations : compte compromis, rançongiciel, fuite, accès non autorisé, perte d'un poste, action anormale d'un agent d'IA, panne grave. Une violation de données personnelles, au sens de l'article 4.12 du RGPD, en est un cas particulier : destruction, perte, altération, divulgation ou accès non autorisé, accidentel ou malveillant.

1.2. Ce que couvre cette page. Les incidents qui touchent nos propres systèmes (postes, comptes, messagerie, Nexus), les systèmes que nous hébergeons ou maintenons pour vous, et ceux que nous découvrons sur vos systèmes pendant une mission.

1.3. Articulation. Cette page précise les articles 8.6, 13.4 et 14.4 des CGV, le point D.7 de leur annexe D et la section 11 de notre politique de données personnelles. Une faille signalée par un chercheur suit la page Signaler une vulnérabilité ; la remise en service suit Continuité et réversibilité ; nos mesures de prévention sont décrites dans Sécurité de l'information.

2. Niveaux de gravité

Chaque incident reçoit un niveau à sa qualification. Ce niveau peut être relevé ou abaissé en cours de traitement ; vous en êtes informé.

NIVEAU	EXEMPLES	POINTS D'ÉTAPE AVEC VOUS
1. Critique	Données personnelles ou confidentielles exposées ou exfiltrées, rançongiciel, compte d'administration compromis, production arrêtée	Au moins deux fois par jour ouvré, jusqu'à la remise en état
2. Élevé	Compte d'utilisateur ou poste compromis sans fuite établie, hameçonnage réussi, service fortement dégradé	Au moins une fois par jour ouvré
3. Modéré	Tentative ciblée bloquée, faille découverte et non exploitée, panne partielle avec contournement	À la clôture

NIVEAU	EXEMPLES	POINTS D'ÉTAPE AVEC VOUS
4. Faible	Événement sans effet : balayage de ports, hameçonnage reçu et non ouvert	Inscrit au journal, mentionné dans le compte rendu de maintenance

2.1. Priorité. Un incident de niveau 1 ou 2 passe avant toute autre tâche de l'équipe. Pierre Marsanne conduit lui-même la réponse à un incident de niveau 1.

2.2. Ce qui déclenche votre information. Un incident de niveau 1, 2 ou 3 qui touche vos données ou vos systèmes vous est signalé dans les délais de l'article 4 ci-dessous.

3. Les étapes, de l'alerte à la clôture

Alerte. Une personne de BONBAY, vous, un fournisseur ou un chercheur signale l'événement à contact@bonbay.fr. Une alerte de nos outils de surveillance suit le même circuit.
Qualification. L'événement est examiné, puis confirmé ou écarté en 8 heures ouvrées au plus, et reçoit un niveau. Une violation de données personnelles n'attend pas cette qualification pour vous être signalée (article 4).
Contention. Isoler les systèmes touchés, couper les accès suspects, changer les mots de passe et clés concernés. Sur vos systèmes, une mesure d'isolement est limitée au nécessaire, tracée et vous est notifiée aussitôt (article 9.4 des CGV).
Conservation des preuves. Avant tout nettoyage, nous copions de manière licite les journaux et éléments utiles, et tenons une main courante horodatée de chaque action et décision.
Information. Vous, la CNIL et les personnes concernées, selon le tableau de l'article 4.
Remise en état. Correction de la cause, restauration depuis une sauvegarde saine si nécessaire, contrôle avant la remise en service.
Rapports et retour d'expérience. Selon les articles 5 et 6.
Clôture. Un incident qui vous concerne n'est clos qu'après la remise du rapport complet et votre accord, ou à défaut de réponse 10 jours ouvrés après cette remise.

Une action anormale d'un agent d'IA suit la même procédure : l'agent est arrêté ou isolé dès que cela peut se faire sans aggraver le dommage, et l'opération n'est pas relancée tant que son issue n'est pas connue (article 8.6 des CGV).

4. Qui prévient qui, et quand

SITUATION	QUI PRÉVIENT	DÉLAI	TEXTE
Incident qui touche vos systèmes ou vos données, sans donnée personnelle	BONBAY vous prévient	Sans délai, au plus tard 24 heures après la confirmation	Contrat

SITUATION	QUI PRÉVIENT	DÉLAI	TEXTE
Violation de données personnelles que nous traitons pour vous	BONBAY vous prévient	Sans délai indu, au plus tard 24 heures après notre prise de connaissance, sans attendre la fin de l'enquête	RGPD, art. 33.2 ; annexe D.7 des CGV
Notification de cette violation à la CNIL	Vous, responsable du traitement, ou BONBAY sur mandat écrit	72 heures après votre prise de connaissance, sauf absence de risque pour les personnes	RGPD, art. 33.1
Information des personnes concernées	Vous, ou BONBAY sur mandat écrit	Sans délai excessif, si le risque est élevé	RGPD, art. 34
Violation touchant nos propres traitements (site, prospects, clients, stagiaires)	BONBAY notifie la CNIL et, si le risque est élevé, les personnes	72 heures après notre prise de connaissance	RGPD, art. 33 et 34
Incident important chez une entité soumise à NIS 2	Vous notifiez l'autorité nationale ; nous vous fournissons les éléments selon l'annexe NIS 2 de votre contrat	Alerte précoce sous 24 heures, notification sous 72 heures, rapport final sous un mois	Directive (UE) 2022/2555, art. 23

4.1. Ce que contient la première information. La nature de l'incident, les catégories et le nombre approximatif de personnes et d'enregistrements concernés, les conséquences probables, les mesures prises ou proposées et le nom de votre contact chez nous, comme l'énumère l'article 33.3 du RGPD. Ce qui n'est pas encore connu est dit comme tel, puis complété à mesure.

4.2. Par quel canal. Par e-mail à l'adresse désignée dans l'annexe D, doublé d'un appel téléphonique pour un incident de niveau 1. Les pièces qui contiennent des données passent par un canal sécurisé, jamais en pièce jointe d'un e-mail.

4.3. Heures calendaires. Le délai de 24 heures court en heures calendaires, week-end compris. Les démarches auprès de la CNIL se font par son service de notification des violations.

5. Rapports écrits

DOCUMENT	DÉLAI	CONTENU
Rapport initial	5 jours ouvrés après la confirmation	Chronologie, périmètre, données et systèmes touchés, mesures prises, questions encore ouvertes
Rapport complet	15 jours ouvrés après la confirmation	Causes profondes, corrections faites, mesures durables avec leur responsable et leur date, retour d'expérience
Suivi des actions	À chaque revue trimestrielle	État de chaque mesure promise, jusqu'à sa clôture

5.1. Pour qui. Les rapports sont rédigés pour vous permettre de remplir vos propres obligations : documentation de la violation, réponse à la CNIL ou à votre autorité sectorielle, information de vos assureurs et de votre direction.

5.2. Ce qu'ils ne contiennent pas. Ni les données d'un autre client, ni les détails techniques qui faciliteraient une nouvelle attaque avant correction ; ces détails vous sont donnés de vive voix, ou par écrit une fois la correction faite.

5.3. Efficacité. Une mesure corrective est vérifiée lors de la revue trimestrielle qui suit sa mise en place ; si elle n'a pas l'effet attendu, elle est reprise et le suivi continue.

---

6. Retour d'expérience, registre et exercices

6.1. Retour d'expérience. Après un incident de niveau 1 ou 2, nous vous proposons une réunion de retour d'expérience avant la remise du rapport complet : ce qui s'est passé, ce qui a fonctionné, ce qui doit changer, chez nous et chez vous. Les leçons sont reportées dans nos procédures et, si besoin, dans une nouvelle version de nos pages.

6.2. Registre des violations. Toute violation de données personnelles, notifiée ou non, est inscrite dans notre registre avec ses faits, ses effets et les mesures prises, comme l'exige l'article 33.5 du RGPD. Les violations survenues sur des données que nous traitons pour vous y figurent aussi. Le registre est conservé 5 ans.

6.3. Exercice annuel. Chaque année, l'équipe joue sur table un scénario d'incident (rançongiciel, fuite de données, agent d'IA qui agit hors de son périmètre) pour vérifier que chacun connaît son rôle et les délais. Le compte rendu alimente la revue annuelle de la sécurité.

6.4. Plainte et signalement. Nous portons plainte lorsque l'infraction le justifie et conservons les preuves à cet effet. La plateforme publique cybermalveillance.gouv.fr oriente les victimes vers une aide.

6.5. Incident chez un fournisseur. Quand OVHcloud, Scaleway, Nexus ou un fournisseur d'IA nous signale un incident qui peut vous concerner, nous vous transmettons ce qui vous concerne dans les mêmes délais, à compter de notre propre information.

---

7. Coûts et responsabilités

7.1. Nos manquements ne vous sont pas facturés. Les corrections qui relèvent d'un manquement de BONBAY ne sont pas facturées comme une prestation supplémentaire (article 8.6 des CGV).

7.2. Assistance hors contrat. Une aide hors du périmètre du contrat, par exemple une enquête approfondie sur vos systèmes ou la reconstruction d'un système que nous ne maintenons pas, vous est chiffrée et n'est engagée qu'après votre accord (article 13.4 des CGV). En urgence, cet accord peut être donné par e-mail.

7.3. Responsabilité. La responsabilité de chaque partie s'apprécie selon son rôle réel, ses obligations et le lien avec le dommage (articles 13.4 et 14 des CGV). L'origine extérieure d'une attaque n'exonère pas BONBAY à elle seule, et aucun délai de signalement de cette page n'éteint vos recours (article 14.4 des CGV).

7.4. Assurance. Nos attestations d'assurance responsabilité civile professionnelle et cyber sont remises sur demande ; les autres documents disponibles sont listés dans Conformité et audits.

---

8. Ce qui dépend de vous, et nos limites

8.1. Vos contacts. Tenez à jour, dans l'annexe D ou le devis, l'adresse et le téléphone de votre contact d'incident, et ceux d'un suppléant. Une information envoyée à un contact périmé fait perdre des heures.

8.2. Vos signalements. Signalez-nous sans retard un incident que vous constatez et donnez-nous un accès sécurisé pour le diagnostiquer (article 14.4 des CGV). Ne relancez pas une opération dont l'issue est inconnue.

8.3. Vos notifications. Pour les données que nous traitons pour vous, la décision de notifier la CNIL et les personnes concernées vous revient, sauf mandat écrit. Nous vous donnons les éléments ; nous ne décidons pas à votre place.

8.4. Ce que nous ne surveillons pas. Sans contrat de supervision, nous ne détectons pas un incident sur vos systèmes : nous le traitons quand il nous est signalé. Sans contrat d'astreinte, la remise en état se fait aux heures ouvrées ; le délai d'information de 24 heures, lui, s'applique toujours.

8.5. Réglementations sectorielles. Si vous êtes soumis à NIS 2, à DORA ou à une autre réglementation de sécurité, les clauses d'incident propres à ces textes figurent dans l'annexe spécifique prévue à l'article 9.6 des CGV. Notre page NIS2 résume ces obligations.

---

9. Contact et mise à jour

9.1. Signaler un incident. Écrivez à contact@bonbay.fr avec en objet « Incident », le système concerné, l'heure du constat et un numéro pour vous rappeler. C'est aussi l'adresse de signalement des failles, reprise dans le fichier https://www.bonbay.fr/.well-known/security.txt.

9.2. Si vous êtes victime ailleurs. Un incident sur un système que nous ne gérons pas peut faire l'objet d'une mission d'assistance ; les premiers gestes sont décrits sur la page Que faire en cas de cyberattaque.

9.3. Version. Version 1.0, en vigueur le 15 novembre 2026. Cette page est revue chaque année (prochaine revue : novembre 2027), à chaque changement important et après tout incident de niveau 1. Un changement qui vous concerne vous est annoncé par e-mail. Les autres engagements

sont réunis sur la page Centre de confiance.