ÊTES-VOUS PRÉPARÉS AU RÈGLEMENT EUROPÉEN SUR LA PROTECTION DES DONNÉES PERSONNELLES ?

Une étude Compuware sur le niveau de préparation des entreprises aux nouvelles obligations instaurées par l'UE en matière de protection des informations personnelles identifiables.

Compuware | The Mainframe Software Partner For The Next 50 Years

Points essentiels à retenir

- Le Règlement Général de l'Union Européenne sur la Protection des Données (RGPD) impose aux entreprises d'effectuer un suivi de toutes les occurrences des données à caractère personnel des clients au sein de leur organisation, d'obtenir le consentement des clients concernant l'utilisation de leurs informations personnelles (y compris le « droit à l'oubli ») et de documenter l'efficacité de cette gouvernance des données pour les auditeurs.
- Deux tiers (68 %) des entreprises risquent de ne pas être en conformité avec le RGPD, en raison d'une augmentation de la collecte des données, de la complexité informatique grandissante, de la multiplicité des applications, de l'externalisation et de la mobilité. Ce risque tient aussi aux politiques laxistes concernant le masquage des données et l'obtention d'une autorisation explicite des clients en matière de données.
- Les entreprises européennes comme américaines doivent, par conséquent, adopter une série de bonnes pratiques, notamment un masquage plus rigoureux des données de test et de meilleurs pratiques concernant le consentement des clients, afin d'éviter des sanctions financières et une altération possible de leur image de marque résultant d'une non-conformité.

Le RGPD et ses implications

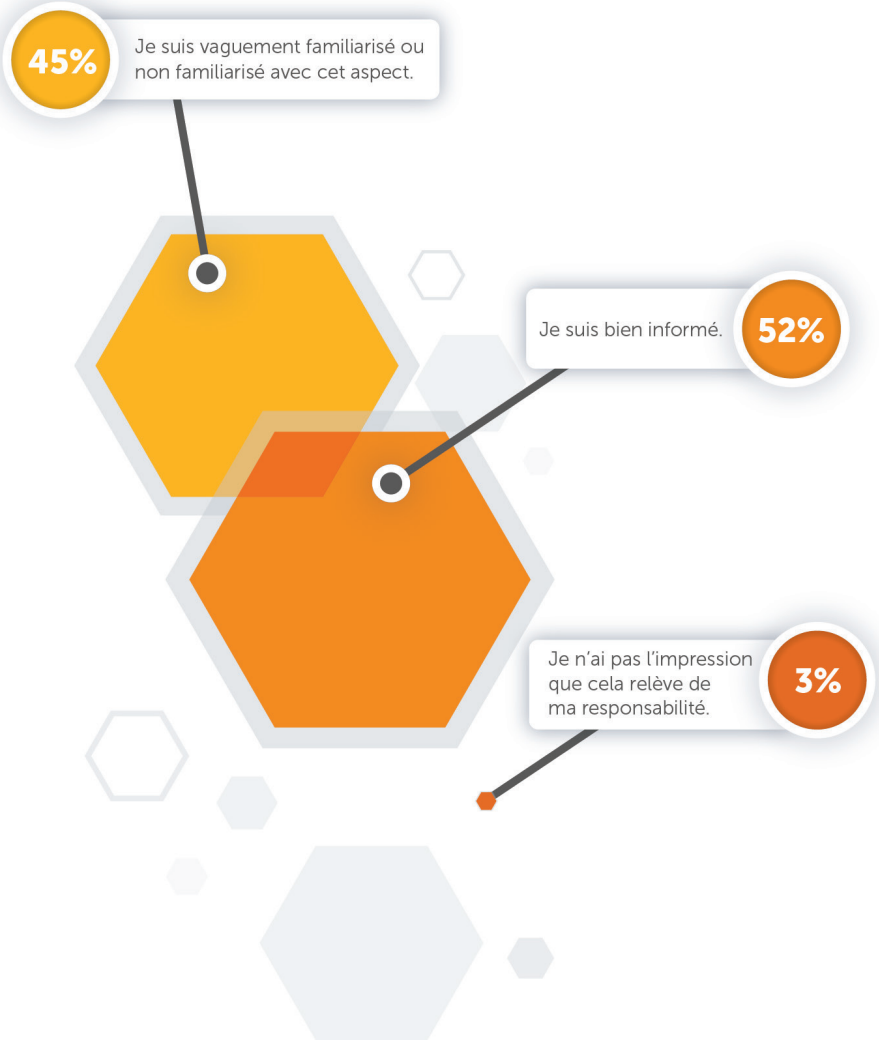
Le RGPD de l'Union européenne a été adopté en avril 2016, afin d'unifier des obligations auparavant réparties à travers différentes juridictions européennes concernant l'utilisation, la gestion et la suppression des informations personnellement identifiables (IPI) des clients par les entreprises. Toutes les entreprises dans l'UE, aux États-Unis et ailleurs, qui collectent des IPI relatives à des citoyens de l'UE, ont jusqu'en mai 2018 pour se conformer à ces dispositions. Tout non-respect du RGPD expose les entreprises à des amendes pouvant atteindre 20 millions € ou 4 % du chiffre d'affaires mondial.

Le RGPD constitue un défi de taille pour les entreprises en matière de gouvernance des données. Elles sont notamment concernées par les dispositions du RGPD qui :

- définissent avec rigueur et de manière vaste les IPI afin d'inclure des aspects aussi divers que les adresses e-mail et numéros d'imposition des clients, ou encore leurs passe-temps et leurs contributions aux réseaux sociaux.
- exigent des entreprises qu'elles obtiennent une autorisation spécifique et explicite d'utilisation des IPI.
- imposent une documentation fiable destinée aux auditeurs et couvrant les mécanismes spécifiques employés par l'entreprise pour le suivi et le contrôle appropriés de l'utilisation des IPI sur tous les systèmes et plates-formes.
- font valoir un « droit à l'oubli » juridique du citoyen de l'UE — autrement dit, exigeant une capacité avérée des entreprises à supprimer, à la demande d'un client, toute occurrence d'information personnelle le concernant sur l'ensemble des systèmes et plates-formes.

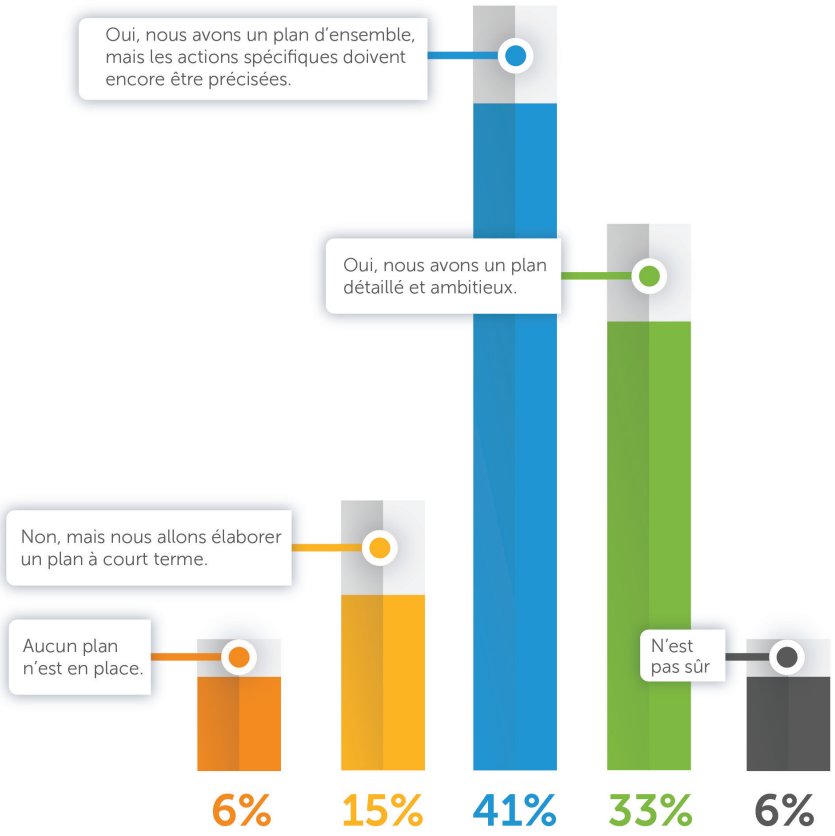
À peine plus de la moitié des répondants (52 %) a déclaré être bien informé sur le RGPD et sur son impact concernant la gestion des données des clients européens. Toutefois, presque autant de répondants (45 %) ont indiqué au contraire qu'ils étaient seulement 'vaguement' familiarisés ou n'étaient pas familiarisés avec les dispositions du RGPD.

À quel point êtes-vous familiarisé avec le règlement général européen sur la protection des données personnelles (RGPD) et avec son impact sur la gestion des données des clients européens par les entreprises ?



La connaissance du RGPD n'est pas en corrélation avec le niveau de préparation. Les deux tiers des répondants (68 %) ont indiqué que leur entreprise n'a actuellement pas de plan complet de conformité au RGPD ou qu'ils ne sont pas sûrs de l'existence d'un tel plan.

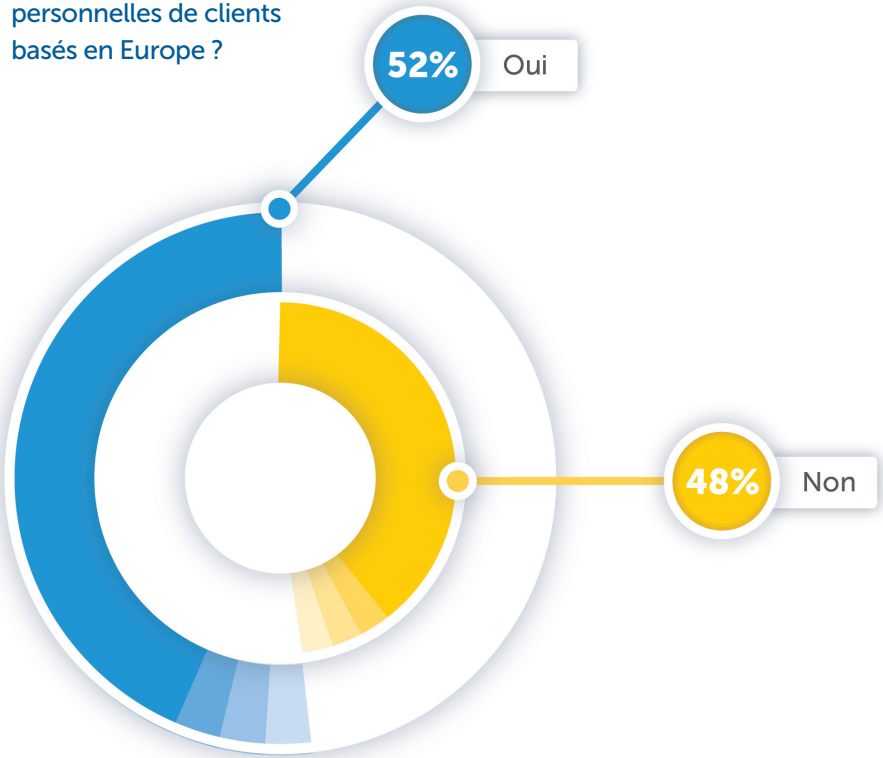
Votre entreprise a-t-elle mis en place des plans d'action en réponse aux implications du RGPD concernant les données des clients ?



Les résultats ont été arrondis au nombre entier le plus proche.

La sensibilisation au RGPD est légèrement inférieure parmi les répondants américains (43 %). Ce manque de sensibilisation pourrait poser des problèmes à de nombreuses entreprises américaines, car 52 % admettent détenir des données de clients de l'UE. Autrement dit, même si elles sont aux États-Unis, elles devront se conformer au RGPD.

Votre entreprise détient-elle ou traite-elle des données personnelles de clients basés en Europe ?



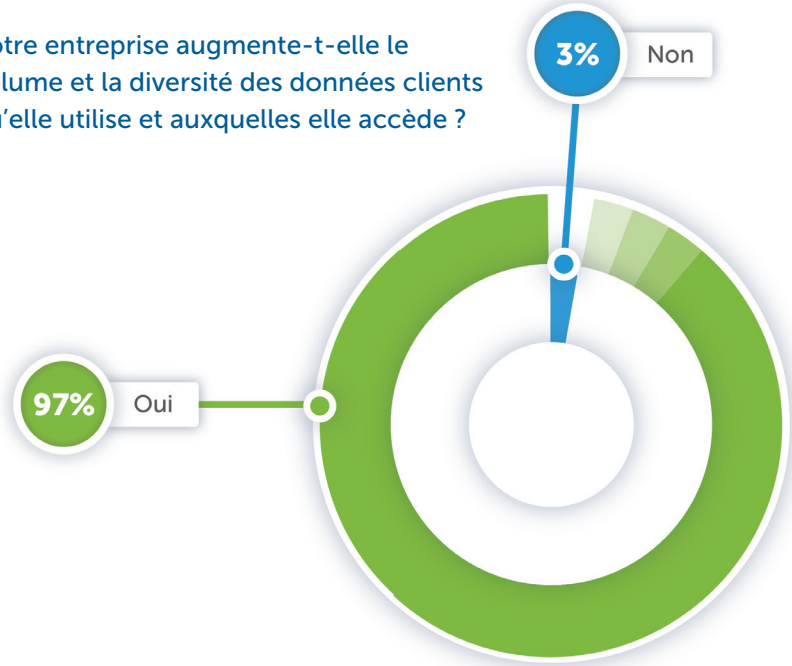
Les défis de la conformité pour les entreprises aux multiples applications

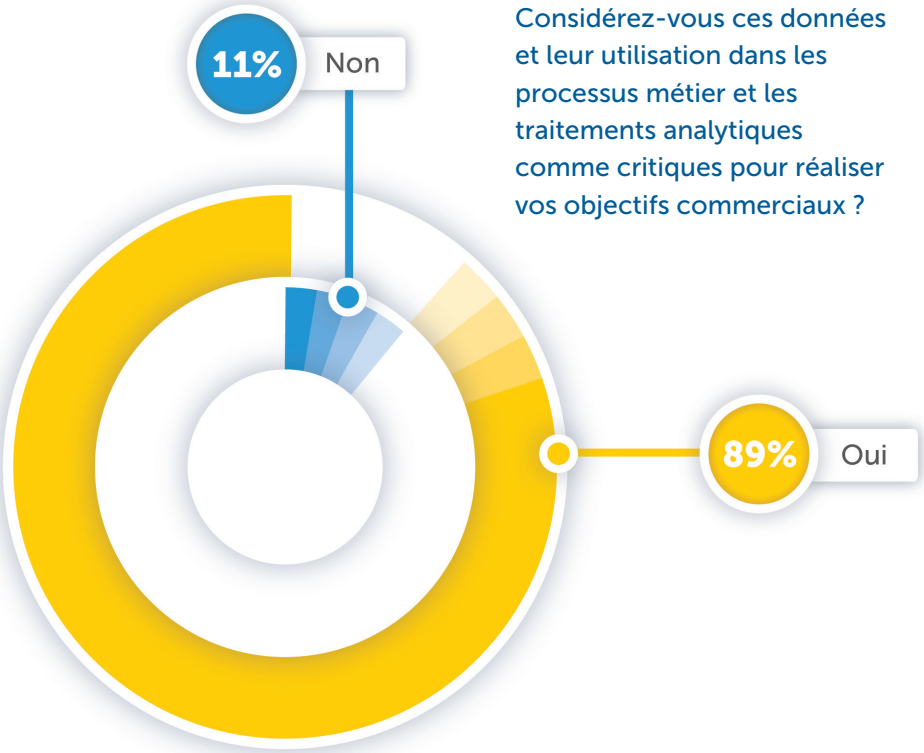
Le respect des obligations du RGPD ne sera pas simple. La nature toujours plus numérique de l'activité économique rend de fait plus difficile la surveillance de chaque occurrence d'information personnelle d'un client. En effet les environnements IT des entreprises englobent de multiples systèmes et plates-formes.

Plus spécifiquement, les répondants ont cité quatre facteurs clés mettant en lumière la difficulté d'un respect du RGPD :

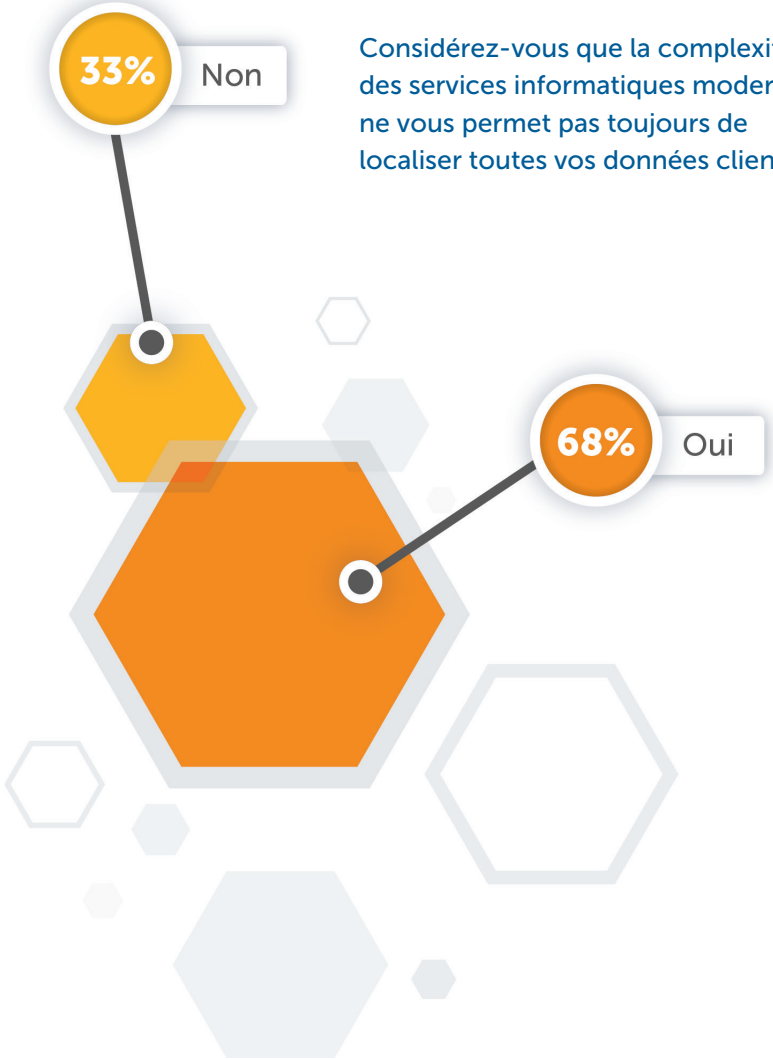
Augmentation de la collecte de données. Plus l'entreprise détient de données, plus le défi de leur suivi est grand et plus il est difficile d'effectuer des opérations spécifiques telles que la suppression d'IPI pour des clients individuels. Néanmoins, les entreprises s'emploient presque toutes (97 %) à collecter encore plus de données clients. Et, dans leur très grande majorité (89 %), elles considèrent ces données comme critiques pour la réalisation de leurs objectifs commerciaux. Par conséquent, toute mesure de respect du RGPD qu'elles adoptent devra être hautement évolutive.

Votre entreprise augmente-t-elle le volume et la diversité des données clients qu'elle utilise et auxquelles elle accède ?





Considérez-vous ces données et leur utilisation dans les processus métier et les traitements analytiques comme critiques pour réaliser vos objectifs commerciaux ?



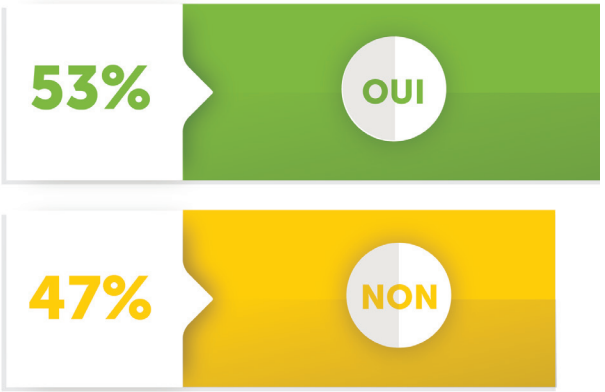
Considérez-vous que la complexité des services informatiques modernes ne vous permet pas toujours de localiser toutes vos données clients ?

Augmentation de la complexité informatique. L'entreprise d'aujourd'hui a généralement accumulé plusieurs générations de technologies, notamment des mainframes, ainsi que des plates-formes distribuées et basées sur le Cloud, dialoguant avec différents types de bases de données et applications. C'est pourquoi 68 % des répondants ont indiqué que la complexité de leurs services informatiques entrave significativement leur aptitude à localiser leurs données à tout moment.

Les résultats ont été arrondis au nombre entier le plus proche.

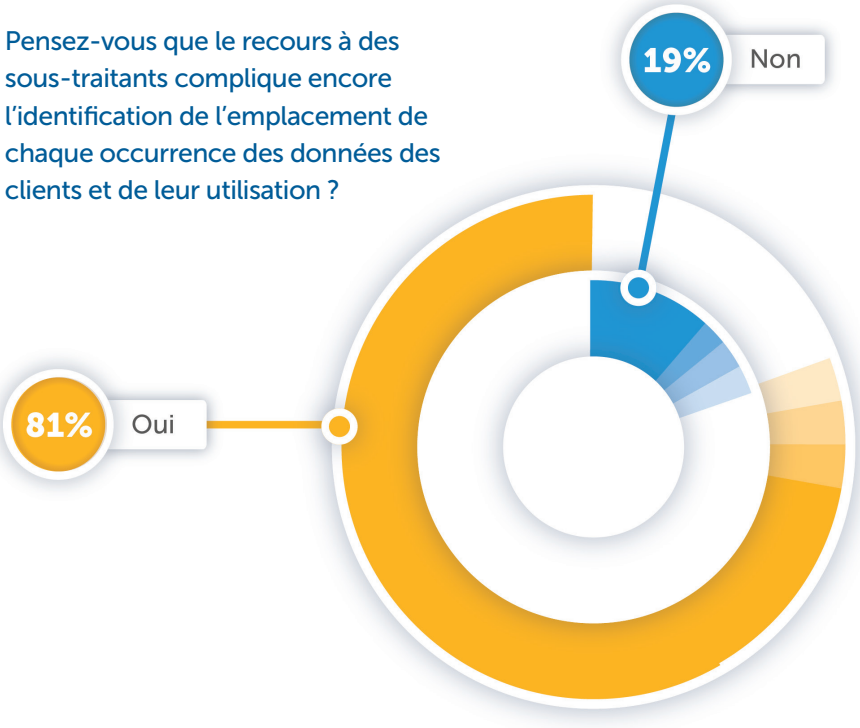
Développement Agile et DevOps. Outre l'évolutivité et la complexité, les entreprises sont aussi confrontées à une évolution et une expansion rapides et inéluctables de leurs environnements numériques. L'adoption du développement Agile et de la culture DevOps est le moteur de cette évolution rapide et continue. Les entreprises cherchent à apporter constamment de nouvelles propositions de valeur originales et concurrentielles sur le marché. En conséquence de quoi, cela rend la conformité au RGPD encore plus difficile pour 53 % des répondants.

Pensez-vous qu'il soit particulièrement difficile de connaître l'emplacement des données de test de votre entreprise à un instant donné ?



Externalisation et mobilité. Le respect du RGPD est encore compliqué car les données des clients ne restent pas toujours au sein de l'entreprise. Les données peuvent être envoyées aux sous-traitants participant au développement des applications et peuvent atterrir sur les périphériques mobiles des utilisateurs. Ces deux problèmes ont été cités par respectivement 81 % et 63 % des répondants. Le Cloud augmente aussi la possibilité d'avoir des données clients à l'extérieur du Data Center de l'entreprise.

Pensez-vous que le recours à des sous-traitants complique encore l'identification de l'emplacement de chaque occurrence des données des clients et de leur utilisation ?

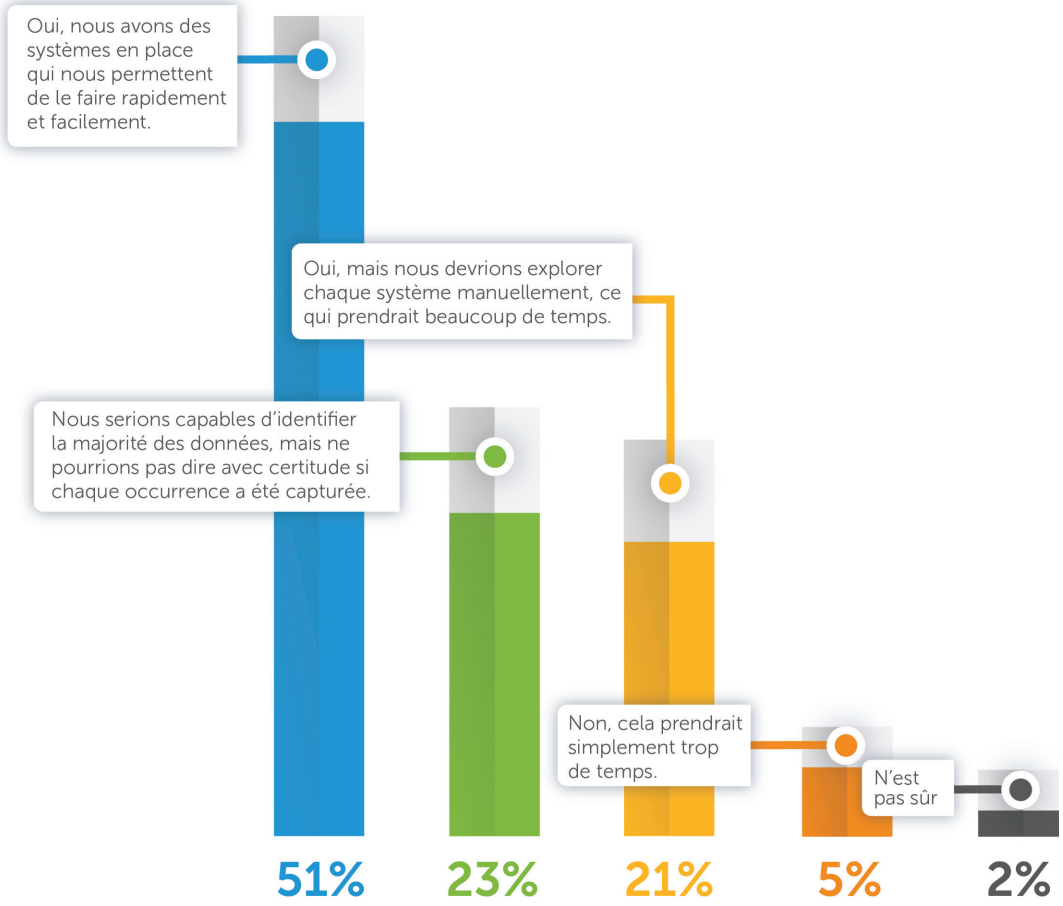


Croyez-vous que la technologie mobile complique davantage le suivi permanent de l'emplacement de vos données clients ?

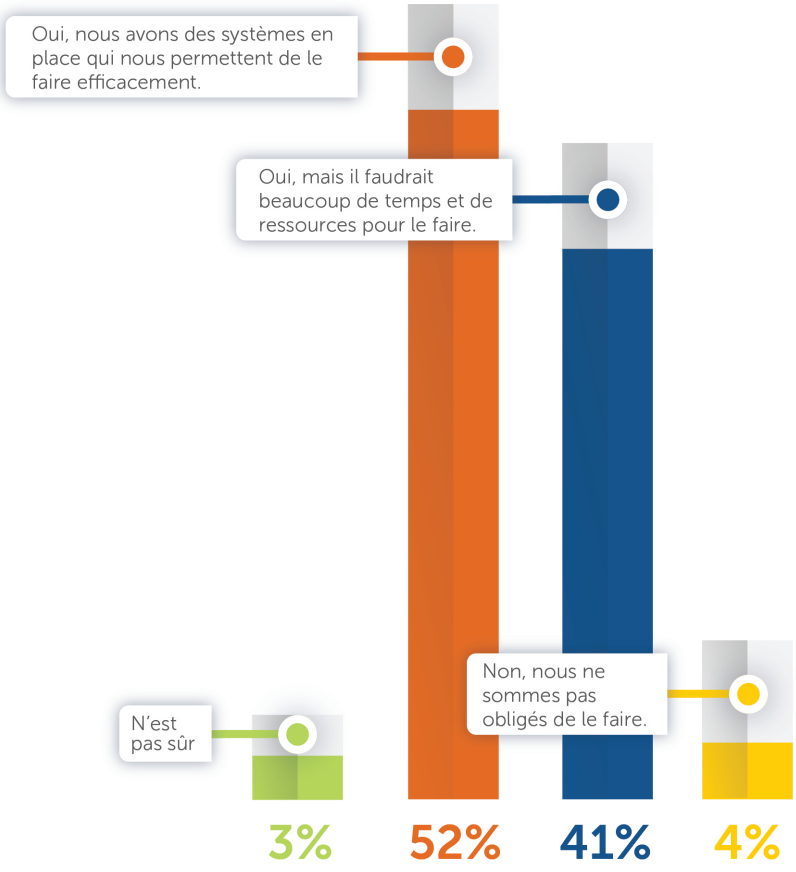
Les résultats ont été arrondis au nombre entier le plus proche.

Du fait notamment de ces facteurs, la moitié seulement (51 %) des répondants est persuadée qu'ils pourraient trouver rapidement et facilement chaque occurrence d'information personnelle d'un client. Près d'un quart (23 %) ont répondu qu'ils ne pourraient pas le faire avec certitude et environ un cinquième (21 %) a indiqué qu'il s'agirait d'un processus manuel nécessitant beaucoup de temps et de ressources. Et seulement une moitié environ (52 %) se montre confiante et affirme pouvoir supprimer toutes les données efficacement en cas de demande dans le cadre du « droit à l'oubli ».

Seriez-vous capable d'identifier et de localiser toute occurrence des données personnelles d'une personne sur vos systèmes ?



Seriez-vous capable de supprimer toutes les données détenues par votre entreprise sur une personne particulière si elle vous le demandait ?



Les résultats ont été arrondis au nombre entier le plus proche.

Données de test et consentement des clients : deux vulnérabilités critiques

L'étude montre aussi deux vulnérabilités critiques, prépondérantes et interdépendantes en rapport avec le respect du RGPD par les entreprises : les données de test et le consentement des clients.

Données de test

Les données de test constituent une vulnérabilité critique et omniprésente en matière de conformité, car elles constituent une des méthodes les plus courantes pour répliquer et transférer des IPI des clients dans l'entreprise. Des jeux de données de test sont régulièrement nécessaires à mesure que les développeurs créent des applications ou améliorent les applications existantes, et ce travail/produit des développeurs doit être testé en permanence en termes d'assurance qualité fonctionnelle et non fonctionnelle. Si les données de test ne sont pas masquées et « anonymisées » correctement, tout nouveau jeu de données de test devient un problème de conformité potentiel dans l'avenir.

Pourtant, malheureusement, 43 % des répondants admettent ou ont un doute sur le fait qu'ils font courir un risque aux IPI des clients en ne garantissant pas l'anonymisation systématique de leurs données avant leur utilisation pour des tests.

Votre entreprise utilise-t-elle l'anonymisation ou d'autres techniques pour dépersonnaliser les données des clients avant de les utiliser dans des environnements de tests ?

L'absence de masquage des données de test crée en fait plusieurs vulnérabilités de conformité, notamment

- L'impossibilité de localiser chaque occurrence d'information personnelle des clients
- L'incapacité à supprimer chaque occurrence d'information personnelle des clients
- L'impossibilité de respecter les exigences de documentation pour les auditeurs concernant ces deux obligations

L'absence de masquage des données clients avant leur partage avec des sous-traitants, qu'il s'agisse de développeurs ou testeurs, présente un risque supplémentaire pour les entreprises car elles sont à la merci des pratiques de sécurité et de conformité du sous-traitant.

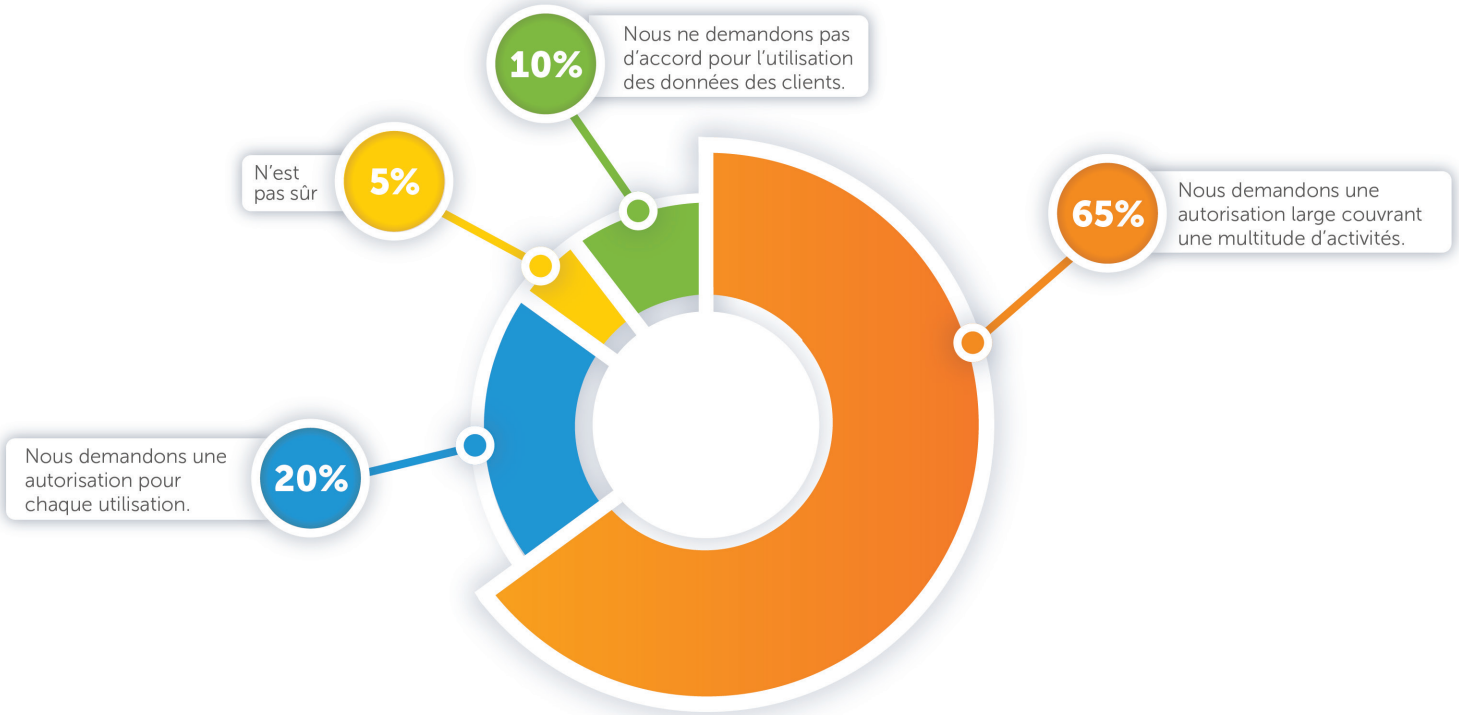
Consentement des clients

Le RGPD accorde aux citoyens de l'UE un plus grand contrôle sur l'utilisation de leurs IPI par les entreprises, en exigeant que celles-ci obtiennent un consentement explicite pour des utilisations spécifiques des IPI, et en permettant aux citoyens de demander la suppression de toutes les occurrences de leurs données personnelles (« droit à l'oubli »).

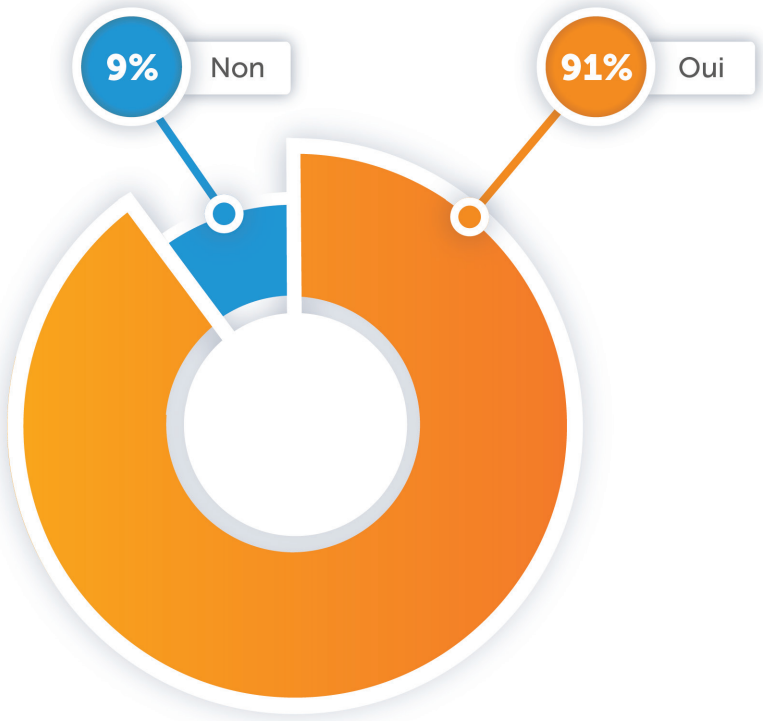
Cela constitue un défi particulier pour les entreprises en matière de données de test, car 80 % des répondants indiquent qu'ils ne demandent pas ou ne sont pas sûrs de demander le consentement explicite des clients pour l'utilisation de leurs données dans les tests d'application. Ce qui constitue actuellement une violation de la législation.

Le masquage et l'anonymisation des données de test résolvent à l'évidence aussi le problème du consentement, car cela les sort du périmètre des dispositions du RGPD sur le consentement relatif aux IPI. Le masquage des données de test constitue aussi une bien meilleure mesure de sécurité que l'approche utilisée actuellement par 91 % des entreprises interrogées et consistant à s'appuyer sur les termes de leurs contrats de travail.

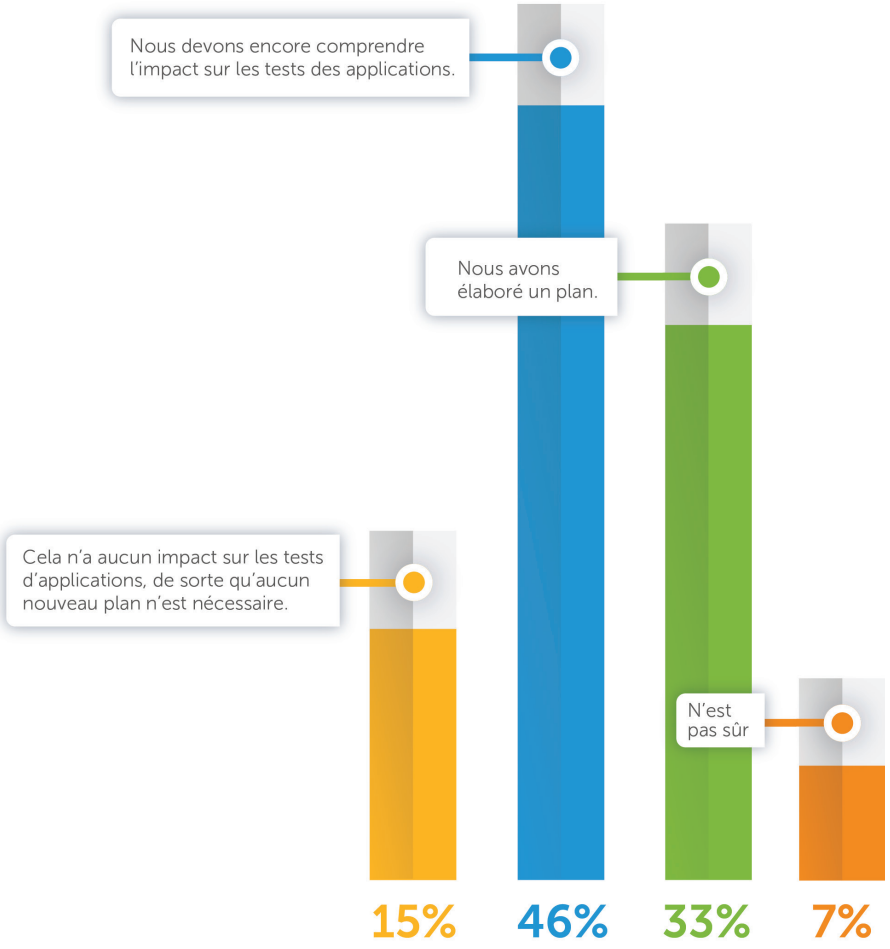
Quelle est votre approche pour obtenir du client l'autorisation d'utiliser ses données personnelles à différentes fins ?



Votre entreprise s'appuie-t-elle sur les termes de ses contrats de travail pour garantir le respect de ses politiques en matière de données lors de leur utilisation à des fins de tests ?



Votre entreprise a-t-elle mis en place des plans pour répondre à l'impact qu'aura le RGPD de l'UE sur sa manière de gérer les données des clients en rapport avec des tests d'applications ?



Les résultats ont été arrondis au nombre entier le plus proche.

Les questions ci-dessus représenteraient un risque plus faible de non-respect du RGPD si les entreprises prenaient déjà les mesures appropriées pour combler leurs lacunes en matière de conformité. Mais elles ne le font pas. Une écrasante majorité de répondants (68 %) n'a pas encore mis en place de plan détaillé pour traiter ces questions. Et 15 % ne sont pas encore sensibilisés au fait qu'il existe des problèmes à résoudre.

Conclusion : Planification, masquage et mise en conformité

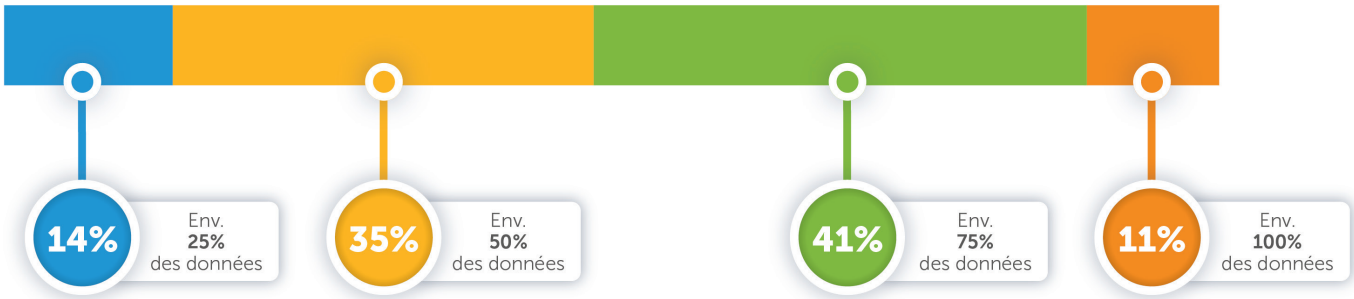
Outre leur aspect descriptif, les résultats de l'étude suggèrent aussi un certain nombre de mesures à prendre :

1. **Informations des personnes concernées par le respect du RGPD.** Les entreprises doivent agir immédiatement pour clarifier leurs obligations découlant du RGPD et informer toutes les personnes concernées (à savoir les développeurs, le personnel de l'assurance qualité et les personnes en charge des sous-traitants) sur leurs responsabilités en matière de respect de ces obligations.
2. **Mise à jour du processus de gouvernance des données et mise en application.** Les personnes concernées doivent déterminer les améliorations nécessaires liées à la gouvernance des données, afin d'assurer un suivi fiable des IPI et de maintenir une corrélation étroite entre l'autorisation du client et l'utilisation effective de ses IPI.
3. **Implémentation de la technologie de masquage.** Il ne suffit pas d'imposer le masquage des données. Si cette approche n'est pas aisée et si elle n'est pas suffisamment sophistiquée pour respecter les exigences techniques des équipes de développement/d'assurance qualité, des IPI non masquées et sans suivi continueront d'être employées dans les environnements de test. La technologie appropriée de masquage des données est donc essentielle pour un respect fiable du RGPD. Le masquage au niveau des mainframes est particulièrement important, car ils contiennent la majorité des données d'entreprise.

Un délai de moins de deux ans est fixé pour la mise en conformité vis-à-vis du RGPD. Et, bien que le respect du RGPD ne soit pas extraordinairement difficile du point de vue technique, les résultats de cette étude indiquent clairement que cela nécessitera des changements significatifs par rapport aux pratiques actuelles des entreprises.

Chaque technologie d'entreprise et chaque responsable de la conformité doivent, par conséquent, initier dès maintenant les premières étapes vers les bonnes pratiques du RGPD. En effet il sera nécessaire de finaliser ce processus avant que les auditeurs commencent à évaluer la conformité et avant que les clients demandent à avoir un meilleur contrôle de leurs IPI.

Quel volume de vos données clients est stocké sur un mainframe ?



Les résultats ont été arrondis au nombre entier le plus proche.

Méthodologie

Cette étude, qui a été réalisée en juin 2016 par la société d'études indépendante Vanson Bourne à la demande de Compuware, a interrogé 400 DSI de grandes entreprises représentatives des marchés verticaux en Europe et aux États-Unis.

The Mainframe Software Partner For The Next 50 Years

Compuware permet aux grandes entreprises du monde entier d'exceller dans l'économie numérique en tirant pleinement parti de leurs investissements à forte valeur ajoutée dans les mainframes. Nous proposons en effet des solutions très innovantes qui permettent aux professionnels de l'informatique ayant des compétences générales de gérer les applications, les données et les opérations sur des plates-formes mainframe.

Pour en savoir plus, rendez-vous sur le site compuware.com.