LEXING
AVOCATS · ADVOCATEN · LAW FIRM

DIGITAL MARKETING CONSULTING
universem

La situation sur le RGPD et les cookies en 2022

Une enquête sur les sites web du Top 100 des entreprises belges

Réalisée par:

Universem SRL & Lexing SRL

La réalisation de ce white paper est le fruit de la collaboration entre Universem et Lexing. En effet, depuis la nouvelle législation RGPD de mai 2018, nous avons constaté une forte augmentation des projets nécessitant une collaboration étroite entre les services marketing et juridique des organisations. Raison suffisante pour, quatre ans plus tard, jeter un coup d'œil sur l'état de la conformité RGPD et l'utilisation des cookies sur les sites Web des 100 meilleures entreprises en Belgique.

Universem

En tant qu'agence spécialisée dans le marketing digital, Universem accompagne ses clients dans l'acquisition, la conversion (drive to store, e-commerce, génération de leads) et la fidélisation web via les pôles suivants :

- Stratégie digitale
- Publicité en ligne et sur les réseaux sociaux
- SEO et Marketing de contenu
- Web analytique et Tableaux de bord

Universem travaille pour de nombreux clients dans différents secteurs, tels que Orange, MeDirect, Camber, Leonidas et WWF.

Plus d'informations ?
www.universem.com

Lexing

Lexing — Belgium est un cabinet d'avocats spécialisés essentiellement en droit des technologies et de l'immobilier. Creactivity, le département IP/IT, conseille notamment les entreprises en matière de traitements de données à caractère personnel, dans les aspects de conformité, contractualisation et défense devant l'APD. Intégré au réseau mondial Lexing, Lexing Belgium dispose de relais spécialisés en droit des technologies sur tous les continents.

En Belgique, Lexing compte une trentaine d'avocats répartis sur quatre implantations : Liège, Namur, Bruxelles et Charleroi.

Plus d'informations ?
www.lexing.be

Introduction

Mai 2018 : Entrée en vigueur du RGPD – Quelle est la situation en 2022 ?

En mai 2018, la législation européenne « RGPD » est entrée en vigueur (Règlement Général sur la Protection des Données, GDPR en anglais pour General Data Protection Regulation). Cette nouvelle loi, liée à la confidentialité des données, a changé la manière dont les données doivent être traitées en ligne en déclarant obligatoire l'ajout de protections par rapport à l'utilisation, au traitement et au stockage des données personnelles.

À la suite de l'évolution des réglementations liées au RGPD et de la sensibilisation grandissante relative aux droits des utilisateurs, le nombre de questions, plaintes et décisions judiciaires en matière de protection des données et de confidentialité a fortement augmenté ces dernières années. Il est donc assez évident que toutes les organisations traitant des informations provenant de l'Union Européenne n'ont d'autre choix que de changer leur façon de collecter et de traiter les données pour se conformer aux nouvelles réglementations.

Chez Universem, en tant qu'entreprise spécialisée en marketing digital, nous sommes constamment amenés à naviguer sur le web dans le cadre de nos fonctions. Au cours de ces navigations en ligne, nous avons constaté qu'une majorité d'entreprises n'avaient toujours pas mis en place suffisamment de contrôles et protections alors que le Règlement Général sur la Protection des Données est entré en vigueur il y a bientôt 4 ans. Nous avons donc décidé de nous associer avec Lexing, un cabinet d'avocats spécialisés essentiellement en droit des technologies et de l'immobilier, afin de réaliser une étude approfondie de la situation en Belgique.

A propos de la recherche

Afin d'évaluer le degré de maturité et de préparation en matière de protection des données des sites web belges, nous avons procédé à une étude de 100 sites web appartenant à des entreprises reprises dans le rapport "Top 5000 biggest Belgian Companies" publié en 2020 par Trends. La sélection s'est effectuée sur base du chiffre d'affaires de la région d'appartenance (10 entreprises par région) et de la présence d'un site internet comportant un « .be »[1].

Sur base d'une série de questions, pondérées en fonction de leur importance dans la législation actuelle, la conformité de chaque site web a été analysée et classifiée en quatre catégories, allant de « Pas du tout conforme au RGPD » à « Entièrement conforme au RGPD ».

L'analyse a été réalisée en janvier 2022. Les principales conclusions de cette recherche ainsi que les résultats détaillés de certaines questions sont à découvrir dans la suite de ce document.

[1] La méthodologie complète est disponible en annexe.

Sommaire

1 Comprendre la notion de «cookies» 7

2 Contexte juridique 9

2.1 Protection de la vie privée 9

2.2 Communications électroniques 10

3 Sanctions 12

3.1 Des pénalités financières s'élevant jusqu'à 4% du chiffre d'affaires mondial 12

3.2 L'image de marque risquant d'être mise à mal vis-à-vis des utilisateurs 13

4 La situation en Belgique: 2/3 des entreprises ne respectent pas la legislation en vigeur ! 14

5 Les «cookies-banner», la solution pour assurer la conformité 16

5.1 Les critères à respecter pour une bannière dite «conforme» 18

5.2 L'importance des politiques de confidentialité et de cookies 21

6 Conclusions et prospectives 22

1. Comprendre la notion de «cookies»

Les cookies ne sont pas qu'un plaisir coupable chocolaté, ils forment aussi un élément technique crucial pour le fonctionnement de l'Internet. Ils sont apparus dans les années 90 afin de donner aux sites web une mémoire que le protocole HTTP ne fournissait pas en lui-même. Les cookies sont de petits fichiers textes que le site web que vous visitez place sur votre appareil lorsque vous naviguez. Le but est que le serveur identifie le cookie lorsque l'usager visite le même site web ultérieurement et qu'il reflète dans la nouvelle session les choix précédents de l'utilisateur : langue de l'interface, panier d'achats, connexion à un compte… Au vu de ces exemples, les cookies semblent faciliter la navigation de l'internaute et donc paraissent inoffensifs. Cependant, ce mécanisme se déroule souvent à l'insu de l'utilisateur, qui ne s'aperçoit pas que ses données sont suivies et sauvegardées ni de l'ampleur des traitements.

On distingue généralement les cookies par leur finalité, leur durée de vie ou leur provenance.

- Les cookies peuvent être indispensables à la bonne navigation sur le site web et à l'utilisation de ses fonctionnalités (« cookies strictement nécessaires »), comme permettre l'accès à une partie sécurisée du site pour réaliser un achat par exemple. Les cookies sont également utilisés pour retenir un choix opéré par l'internaute (« cookies fonctionnels »), comme la conservation d'un panier d'achats ou la langue de navigation. Les cookies peuvent aussi collecter des informations sur la façon dont un site est utilisé (« cookies analytiques ») ou suivre la navigation à travers le web à des fins de marketing (« cookies publicitaires »). Finalement, les cookies peuvent être déposés par les médias sociaux (« cookies réseaux sociaux ») dans le but de permettre à l'utilisateur de partager du contenu avec son réseau.

- Les cookies peuvent être temporaires et effacés lors de la fermeture du navigateur (« cookies de session ») ou subsister sur le terminal de l'internaute (« cookies persistants ») jusqu'à leur expiration, ou leur suppression par l'utilisateur.
- Enfin, les cookies peuvent être implantés par le gestionnaire du domaine directement (« first-party cookies ») ou par un tiers (« third-party cookies »), éventuellement par le biais de boutons, de plug-ins ou d'images incorporées au site web.

Ce sont généralement ces cookies, installés par des tiers, qui sont pointés du doigt. Par leur omniprésence sur le web, les cookies tiers récoltent des quantités importantes de données.

Grâce à la combinaison du suivi et du profilage, les cookies sont à ce jour le moyen le plus utilisé pour suivre le parcours des utilisateurs en ligne et exposer des messages ciblés. Il existe aujourd'hui tout un écosystème construit autour des données collectées grâce aux cookies, allant du marketing en ligne, où ils permettent de faire correspondre les profils avec les clients types des entreprises dans les espaces publicitaires, au suivi du parcours des utilisateurs via les outils d'analyse. Grâce à cette vue d'ensemble fournie par les informations collectées, les cookies sont utiles dans l'optimisation de la stratégie digitale des entreprises. Cet écosystème dépasse même le cadre du marketing en ligne puisqu'il permet également de faire évoluer en permanence les services web en fonction des retours des usagers.

2. Contexte juridique

De nombreuses personnes et sociétés l'ignorent vu l'ubiquité des cookies, ou ne s'estiment pas concernées vu leur taille. Cependant, étant donné les informations que les cookies peuvent contenir, leur utilisation est encadrée juridiquement. Le non-respect des règles est sanctionné et certaines décisions ne concernent pas que des GAFA, mais bien des PME locales.

Juridiquement, les cookies sont considérés d'une part sous l'angle des traitements de données à caractère personnel qu'ils entraînent, d'autre part, sous l'angle des communications électroniques dont ils sont une composante. Les traitements de données à caractère personnel générés par les cookies doivent respecter les règles en matière de RGPD. L'installation des cookies et leur utilisation doit correspondre aux exigences de la loi ePrivacy. Les deux régimes juridiques se superposent sans se confondre malgré leurs points communs, ils doivent donc être respectés tous les deux.

2.1 Protection **de la vie privée**

Les cookies sont utilisés pour récolter différents types d'informations. Ils peuvent inclure des données classifiées comme purement techniques jusqu'à des données à caractère personnel. Dans ce dernier cas, les exploitants de ces données doivent respecter le Règlement Général sur la Protection des Données (RGPD). Ce règlement, entré en vigueur dans l'Union Européenne en mai 2018, fournit le cadre juridique applicable aux traitements de données à caractère personnel. L'objectif est que les entreprises mettent en place des

garanties techniques et opérationnelles pour la protection des données qu'elles contrôlent. Toute entreprise qui traite des données relatives à des citoyens de l'Union Européenne se doit de se conformer à ce règlement. En général, respecter ces obligations implique de fournir une information préalable claire et complète à l'internaute et, dans une grande partie des cas, la collecte d'un consentement de qualité sur les traitements effectués. Le consentement n'est toutefois qu'une des bases légales possibles pour les traitements. Les cookies nécessaires et fonctionnels peuvent, par exemple, opérer sur d'autres bases légales, comme l'intérêt légitime ou l'exécution d'un contrat.

2.2 Communications **électroniques**

La directive ePrivacy de 2002 vise les cookies et les dispositifs de suivi similaires implantés sur le terminal d'un utilisateur. En termes généraux, elle prévoit que l'usage de cookies exige une information préalable et une possibilité de s'opposer au traitement, sauf pour les opérations strictement nécessaires à la fourniture du service demandé par l'internaute.

Cette directive a été transposée en droit belge par la loi dite « communication électronique » de 2005. La loi belge va plus loin que la directive « ePrivacy » en ce sens qu'elle impose un consentement informé et exprès de l'internaute avant l'installation des cookies sauf, à nouveau, pour les opérations strictement nécessaires à la fourniture du service demandé par l'internaute. Le consentement doit pouvoir évidemment être retiré à tout moment aisément.

Les exigences pour s'assurer de la qualité de ce consentement sont très hautes, puisque la Cour de Justice a décidé que les critères devaient être les mêmes que ceux appliqués par le RGPD, soit un consentement préalable, informé, spécifique, libre et non ambigu.

Pull Strategy
Teamwork
Efficient
organisation
Customer
Relationshi
uni
ver
sem

3. Sanctions

3.1 Des **pénalités financières** s'élevant jusqu'à 4% du chiffre d'affaires mondial

Les manquements à la loi sur les communications électroniques et les infractions au RGPD sont passibles de sanctions administratives et pénales. Le RGPD est connu pour prévoir des pénalités importantes, pouvant s'élever à 4 % du chiffre d'affaires mondial du groupe auquel la société punie appartiendrait.

Concrètement, les autorités nationales de protection des données (APD) sont de plus en plus attentives au respect du droit de la vie privée. La surveillance du marché du marketing en ligne fait partie des priorités des différentes autorités nationales. Et les cookies sont un sujet chaud :

- En 2020, l'APD belge a condamné un site web d'information juridique à 15 000 EUR d'amende pour sa mauvaise politique d'utilisation de cookies.

- En 2021 en France, la CNIL — l'autorité française — a condamné un journal à une pénalité de 50 000 EUR en raison du dépôt de cookies publicitaires à partir de son site web sans recueil du consentement préalable des internautes.

Ces deux sanctions concernaient des PME nationales, mais les acteurs importants commencent également à sentir le souffle des régulateurs.

Début 2022, les autorités nationales autrichienne et française ont épinglé Google Analytics, poids lourd de l'écosystème des outils d'analyse, pour des transferts de données vers les USA contraires aux exigences du RGPD.

L'APD belge vient également de condamner à une amende de 250.000 EUR un acteur majeur de la publicité en ligne, qui édicte une norme employée pour obtenir et propager les autorisations concernant l'installation et l'usage de traceurs publicitaires comme les cookies. Des manquements aux obligations de transparence et d'informations des utilisateurs leur sont reprochés.

3.2 **L'image de marque** risquant d'être mise à mal vis-à-vis des utilisateurs

Outre les sanctions financières, les sanctions relatives à l'image de marque sont également à prendre en compte. Les consommateurs sont de plus en plus conscients de leurs droits et ne se font pas prier pour le faire savoir.

L'Autorité de protection des données en Belgique (ADP) a noté une augmentation du nombre de plaintes concernant des fuites de données, allant jusqu'à au moins 1885 plaintes en 2021 contre 668 en 2020.

"L'augmentation du nombre de plaintes reçues montre malgré tout que les citoyens sont de plus en plus sensibles à la protection de leurs données"

Aurélie Waeterinckx, porte-parole de l'Autorité.

Tous ces éléments sont autant de signaux qui montrent que les cookies sont dans le collimateur des acteurs du secteur et des utilisateurs et que les entreprises – quelles que soient leur taille et leur degré de technicité – doivent se mettre en ordre.

4. La situation en Belgique: 2/3 des entreprises ne respectent pas la legislation en vigeur !

Dans le cadre de notre recherche et sur base d'une série de questions, pondérées en fonction de leur importance dans la législation actuelle, chaque site web analysé a obtenu un score sur 18. A partir de ce score, quatre catégories de conformité ont été définies. Cette échelle a été réalisée dans le but de classifier les sites du plus conforme au moins conforme, en prenant en compte l'existence de certains flous juridiques, pouvant être qualifiés de « zones grises ».

Les quatre degrés de conformité définis sont les suivants :

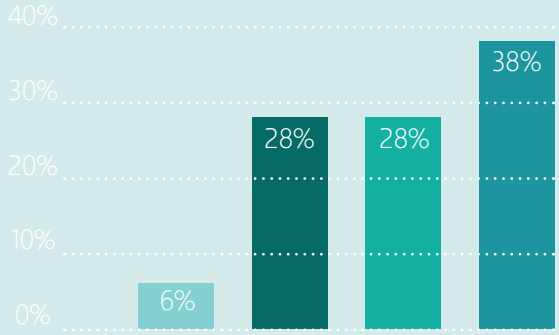
- Entièrement conforme au RGPD (strictement supérieur à 15.5 sur 18)
- Partiellement conforme au RGPD (strictement supérieur à 11.5 et inférieur ou égal à 15.5, sur 18)
- Peu conforme au RGPD (strictement supérieur à 6.5 et inférieur ou égal à 11.5, sur 18)
- Pas du tout conforme au RGPD (inférieur ou égal à 6.5, sur 18)

La conclusion principale de notre analyse est que la législation n'est pas totalement suivie et mise en pratique par les entreprises, pourtant leaders sur le marché belge.

En effet, seuls 6% des sites analysés sont totalement conformes au RGPD et 28% le sont partiellement. Cela signifie que 34% des entreprises suivent la majorité des règles édictées et tentent de placer la protection des données de leurs utilisateurs en tête de leurs préoccupations.

Par ailleurs, 28% des sites analysés sont peu conformes au RGPD et 38% ne le sont pas du tout. Cela signifie que 66% - une majorité - des entreprises ne considèrent pas la législation en la matière comme étant l'une de leurs préoccupations majeures. Les hypothèses avancées sont la mauvaise compréhension des protections et configurations à mettre en œuvre afin de devenir pleinement conforme ou le manque de considération du sujet, pourtant primordial dans la situation actuelle.

Niveau de conformité au RGPD

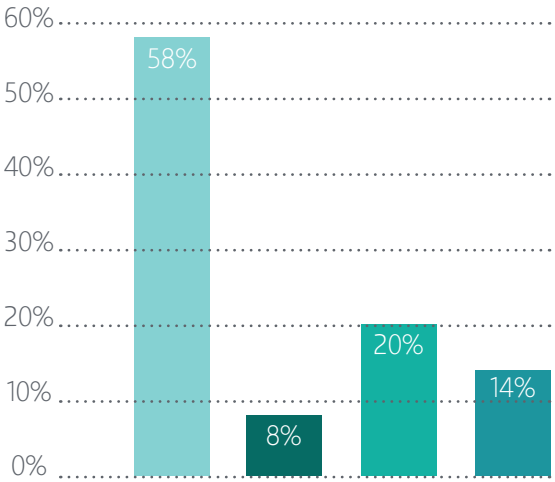


- Entièrement conforme au RGPD
- Peu conforme au RGPD
- Partiellement conforme au RGPD
- Pas du tout conforme au RGPD

5. Les «cookies-banner», la solution pour assurer la conformité ?

Après l'entrée en vigueur de la directive ePrivacy et celle du Règlement Général de la Protection des Données, les sites web européens ont vu fleurir des bannières, et autres pop-ups, concernant les cookies. Il ressort de notre étude qu'une large part (86%) des sites web analysés sont dotés d'une bannière relative aux cookies. Certaines de ces bannières se contentent d'avertir l'internaute : s'il poursuit sa visite, des cookies seront installés (« bannière informative »). D'autres offrent la possibilité de refuser ou d'accepter tous les cookies en un clic (« bannière à niveau de consentement unique »). D'autres encore sont plus avancées et proposent une sélection, quelquefois très granulaire, des types de cookies autorisés (« bannière à niveau de consentement multiple »).

Type de bannières affichées



- Bannière à niveau de consentement multiple
- Bannière à niveau de consentement unique
- Bannière informative
- Aucune bannière

Toutefois, être doté d'une bannière est un début mais n'est pas suffisant pour respecter l'intégralité des règles relatives à la directive ePrivacy et au RGPD

5.1 Les critères à respecter pour une bannière dite « conforme »

Tout d'abord, pour être conformes et permettre l'enregistrement licite des cookies non nécessaires, les « cookies-banner » doivent respecter un certain nombre de critères :

La bannière doit être visible. D'après notre recherche et nos critères relatifs à la visibilité, un bon tiers (35 %) des bannières sur les sites analysés ne sont pas suffisamment visibles. Celles-ci sont parfois placées via un fin bandeau en bas de page, utilisent de petits caractères et / ou encore affichent des couleurs peu apparentes.

Le consentement doit se manifester par une démarche active.

- Le consentement ne peut pas être déduit du fait que l'internaute continue la navigation ou que l'internaute ait paramétré son navigateur pour approuver les cookies. Les bannières dites informatives ne sont donc pas conformes lorsque le consentement de l'utilisateur est requis.
- Une case cochée par défaut ne constitue pas un consentement valide. Ce critère semble bien connu de tous : 90% des sites analysés et possédant une bannière avancée affichent des catégories de cookies non sélectionnées par défaut.

Le consentement doit être libre.

- Cela signifie que la présentation de la bannière ne doit pas induire l'accord et doit proposer un choix clair. Il arrive que des bannières soient présentées de manière à favoriser ou à induire l'accord de l'internaute, c'est ce qu'on appelle les « dark patterns ». De nombreux designs montrent un grand bouton vert « J'accepte » et un lien discret, dans une police de taille inférieure, « Plus d'information ». Ces designs sont hautement critiquables. Parmi les sites analysés disposant d'une bannière, 46% d'entre eux n'offrent pas la possibilité de rejeter les cookies directement sur la bannière, ce qui signifie qu'il n'est pas aussi facile de

rejeter que d'accepter les cookies et que l'utilisateur peut être influencé dans son choix.

- La liberté implique également la possibilité de refuser sans perdre un avantage. L'installation des cookies ne peut pas conditionner l'octroi d'un service. Par exemple, l'exploitant du site web « gratuit » dont le business model est basé sur la publicité personnalisée doit proposer une alternative à l'internaute qui rejette un cookie non nécessaire. De plus en plus de « cookie paywall » apparaissent d'ailleurs pour fournir une autre version du site, payante et sans pistage.

Le consentement doit être spécifique, c'est-à-dire être accordé pour des traitements précis. Il ne suffit pas de donner une permission générale, globale et non définie.

Le consentement doit être informé.

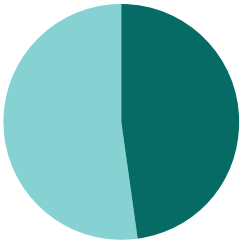
- Avant de cliquer, l'internaute doit avoir eu la possibilité d'être renseigné sur le responsable du traitement, les finalités poursuivies par les cookies, les données qu'ils collectent et leur durée de vie. Selon notre étude, 57% des sites qui disposent d'une bannière font directement mention de leurs cookies. Les différentes catégories de cookies utilisées et leurs objectifs sont quant à eux évoqués dans les paramètres de préférence de la bannière. Le nombre de sites qui liste les cookies et mentionne leur durée de vie est encore plus faible. A ce sujet, l'Autorité de Protection des Données (APD) favorise l'indication en différentes couches, afin que l'internaute puisse être prévenu à un niveau de détail qui lui convient.

- L'information doit également porter sur les droits que le RGPD accorde aux personnes concernées.

- Enfin, l'exploitant doit porter attention à la présentation et à la rédaction, de sorte qu'elle soit complète, compréhensible et non trompeuse.

En ce qui concerne le côté plus technique, le moment où le cookie est déposé sur l'appareil du visiteur est extrêmement important dans la législation actuelle. Aucun cookie non nécessaire ne peut être installé avant l'interaction avec la bannière et la confirmation du consentement de l'internaute. Néanmoins, nous constatons que 48% des sites qui ont une bannière déclenchent les cookies avant même que l'utilisateur n'ait effectué un choix. C'est donc une problématique majeure impactant négativement l'attribution du score aux différents sites analysés.

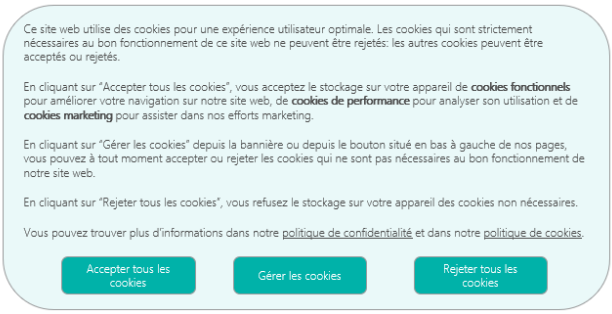
Configurations techniques des cookies



Cookies déclenchés avant le consentement

Cookies déclenchés après le consentement

Exemple



Ce site web utilise des cookies pour une expérience utilisateur optimale. Les cookies qui sont strictement nécessaires au bon fonctionnement de ce site web ne peuvent être rejetés: les autres cookies peuvent être acceptés ou rejetés.

En cliquant sur "Accepter tous les cookies", vous acceptez le stockage sur votre appareil de **cookies fonctionnels** pour améliorer votre navigation sur notre site web, de **cookies de performance** pour analyser son utilisation et de **cookies marketing** pour assister dans nos efforts marketing.

En cliquant sur "Gérer les cookies" depuis la bannière ou depuis le bouton situé en bas à gauche de nos pages, vous pouvez à tout moment accepter ou rejeter les cookies qui ne sont pas nécessaires au bon fonctionnement de notre site web.

En cliquant sur "Rejeter tous les cookies", vous refusez le stockage sur votre appareil des cookies non nécessaires.

Vous pouvez trouver plus d'informations dans notre politique de confidentialité et dans notre politique de cookies.

Accepter tous les cookies | Gérer les cookies | Rejeter tous les cookies

Chez Universem, nous répertorions et documentons tous les cookies que vous placez sur votre site Web et identifions quels cookies peuvent être considérés comme « risqués » en termes de respect de la confidentialité des données. Si vous ne possédez pas encore de bannière de gestion des cookies sur votre site web, nous implémentons cette bannière via une plateforme

spécifique. Avec votre soutien et celui de votre représentant légal, nous personnalisons la façon dont vous collectez et analysez les données pour vous assurer que les configurations soient conformes aux recommandations de votre représentant légal. En configurant votre site par rapport aux réglementations légales, vous pouvez continuer à optimiser votre stratégie sur base de vos données en toute légalité.

5.2 L'importance des politiques de confidentialité et de cookies

Enfin, la bannière de cookies n'est qu'un aspect de la conformité aux règles en matière de protection des données à caractère personnel. Les sites web devraient également contenir des informations plus générales sur les traitements de données opérés. Sur ce point, les résultats de l'étude sont plutôt optimistes puisqu'il en ressort que la majorité des entreprises analysées sont conscientes des règles en matière de protection des données des utilisateurs et elles le mentionnent explicitement sur leur site. 79% des entreprises présentent une politique de confidentialité sur leur site internet et 63% proposent une politique de cookies. Il est donc évident que la protection des données est au cœur de nombreuses discussions internes et ce, même si l'ensemble des règles n'est pas respecté. Malgré tout, il est important de spécifier que la présence d'une politique de confidentialité n'implique pas forcément la présence d'une politique en matière de cookies et vice versa.

Creactivity, le département IP/IT de Lexing, conseille notamment les entreprises en matière de traitements de données à caractère personnel, dans les aspects de conformité, contractualisation et défense devant l'APD. Intégré au réseau mondial Lexing, Lexing Belgium dispose de relais spécialisés en droit des technologies sur tous les continents et peut donc vous accompagner dans votre mise en conformité.

6. Conclusions et prospectives

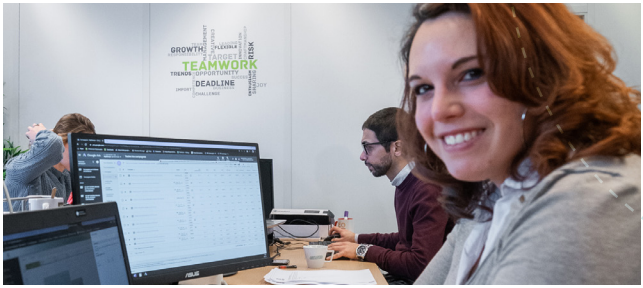
Avec 2/3 des entreprises qui ne respectent pas totalement la législation actuelle en vigueur, cette étude démontre que la situation du marché belge doit encore être améliorée en ce qui concerne la conformité aux règles en matière de protection des données. En tant qu'entreprise opérant et traitant des données provenant de l'Union Européenne, si vous n'avez pas encore pris le sujet en main, il est nécessaire de commencer les démarches concernant votre mise en conformité. Dans le cas où vous auriez déjà mis en place des configurations, il est également important de suivre l'évolution de la situation afin de vous assurer une totale conformité à tout moment.

Nous avons vu que les autorités de protection des données font de la surveillance de la conformité du marketing digital, des outils d'analyses et des cookies une priorité. Les risques d'enquête et de sanctions sont bien réels, et ce pour toutes les entreprises, de la multinationale à la TPE. La lecture de la législation sur la vie privée par l'APD et ses consœurs européennes évolue rapidement. Cela implique des changements sur les sites des entreprises qui doivent s'adapter en parallèle de ces évolutions rapides.

Au-delà des risques de sanctions pour non-conformité, les entreprises ne doivent pas perdre de vue que les internautes sont de mieux en mieux informés de leurs droits et sensibles au respect de leur vie privée. La transparence à ce niveau est une valeur porteuse pour l'image de marque des entreprises.

En ce qui concerne le cadre juridique, une proposition de nouveau règlement ePrivacy pour remplacer la directive a été publiée en 2017. En choisissant le règlement, l'UE souhaitait garantir un régime harmonisé entre tous les États membres. Le texte est actuellement dans la phase finale des négociations. Le projet contient plusieurs dispositions qui auront un impact sur les cookies ainsi que sur le secteur AdTech qui s'appuie sur cette technologie de traçage.

À ce stade, il est délicat de se prononcer sur la version ultime, mais il semble déjà acquis que ce règlement se focalisera sur des solutions techniques, passant par la configuration des navigateurs et la création d'un mode « Do not track » sur ceux-ci. Par ailleurs, les compétences des autorités de protection de données devraient être étendues aux aspects « communications électroniques » lorsqu'il s'agira de vérifier et de sanctionner les outils de pistage des internautes, comme les cookies.



Des questions?

Vous souhaitez mettre à jour ou développer votre conformité à la protection des données ?

Ce livre blanc est une co-production d'Universem et de Lexing.

Pour toute question concernant votre site Web (technique, suivi, analyse) ou liée à vos projets digitaux, veuillez contacter Universem.

www.universem.com
marketing@universem.com

Pour toute question concernant les aspects juridiques des thèmes abordés dans ce livre blanc, veuillez contacter Lexing

www.lexing.be
brussels@lexing.be

Gembloux

Parc Créalys
Rue Camille Hubert, 13
5032 Gembloux
+32 (0)81 713 430

Bruxelles

Rue Haute, 139/6
B-1000 Bruxelles-Brussel
Tél. +32 2 381 11 91
brussels@lexing.be

Bruxelles

Herrmann-Debrouxlaan, 40
1160 Oudergem
+32 (0)2 318 23 90

Paris

Rue du Helder, 5
75009 Paris
+33 (0)1 86 95 89 29

/universem

© 2020 Universem srl - bv | Universem sarl | www.universem.com

Methodologie - uitgebreide versie (in het engels)

Research problem: Analyse different websites to evaluate the position of Belgian companies in terms of GDPR regulation.

Step 1: Determination of 100 websites for the study

The sample of websites used for this research is based on the 'Top 5000 biggest Belgian Companies' published in 2020 by Trends Top. Among them, 100 companies have been selected. Selections have been made depending on company's revenues (biggest as possible), the Belgian Region (10 companies per region) and the presence of a ".be" website.

Step 2: Development of the questions and field of study

Different questions have been developed in order to determine the level of GDPR compliancy of each selected company. These questions are based on the current regulation, developed by Universem and Lexing.
Here are the different questions:

- Does the website display a cookie banner?
- Is there a reject notion on the banner?
- Is the banner sufficiently visible?
- Does the banner block the interaction with the website?
- Does the banner include the listing of different cookies used and their explanation?
- Does the banner indicate how to manage the cookie settings?
- Does the "reject" and "accept" buttons have the same design?
- Are the banner cookie parameters checked or unchecked by default?
- Is there a cookie policy on the website?
- Is there a privacy policy on the website?
- Does the banner display a link towards the cookie policy and/or the priva-

cy policy?
- How are cookie settings configured? (before or after the consent)
- Does the user have the possibility to update his consent at any moment?

Step 3: Ranking of the level of GDPR compliancy

Each question is rated depending on its degree of importance related to the GDPR legislation.

The final grade is on 18 and responds to four degrees of compliancy.
- Fully GDPR compliant
- Partly GDPR compliant
- Not really GDPR compliant
- Not GDPR compliant

This scale is based on researchers' determination and opinions with a quantitative aspect of the current GDPR Regulation (2021). This study is based on data but also on grades attributed by the research team. Therefore, it might represent a perception bias. It is essential to read this analysis keeping in mind that the participation and perception of each person cannot be neglected.