PREISKEL & CO

CONTROLES DE CONFORMITE AU RGPD
GDPR COMPLIANCE AUDITS BY DPAS

COMMENT SE PREPARER AU CONTROLE D'UNE AUTORITE DE PROTECTION DES DONNEES ?

- Depuis l'entrée en application du RGPD le 25 mai 2018, les pouvoirs des autorités européennes en charge de la protection des données se sont élargis.
- Elles peuvent effectuer des contrôles sur place, sur pièces, sur audition ou en ligne auprès de l'ensemble des responsables de traitement (entreprises privées, associations, collectivités territoriales, administrations publiques) et des sous-traitants pour vérifier la bonne application de la réglementation sur la protection des données personnelles.
- A l'issue de missions de contrôle ou sur plaintes, elles peuvent prononcer des sanctions à l'encontre des responsables de traitement ou des sous-traitants qui auraient commis des manquements à la réglementation sur la protection des données personnelles.
- Notamment, elles peuvent prononcer une sanction pécuniaire d'un montant pouvant aller jusqu'à 20 millions d'euros ou, dans le cas d'une entreprise, 4% du chiffre d'affaires mondial, le montant le plus élevé étant retenu. Cette sanction peut être rendue publique.

Les membres du réseau Lexing® dressent un tableau de la situation actuelle à travers le monde. Les pays suivants ont contribué à ce numéro : Afrique du Sud, Allemagne, Belgique, France, Hongrie, Italie, Grèce.

HOW TO BE PREPARED FOR A GDPR AUDIT?

- *Since the GDPR started to apply on 25 May 2018, the powers of the European data protection authorities (DPAs) have been extended.*
- *They may carry out audits that may take various forms (onsite audit, desk audit, hearing, online audit) on the processing carried out by controllers (private-law bodies, associations, local government authorities, public-law bodies) and processors to verify the proper application of the applicable laws and regulations on the protection of personal data.*
- *If the audit reveals an infringement or in case a complaint is filed, DPAs may impose penalties on controllers and/or processors.*
- *In particular, they may impose a financial penalty of up to €20 million or, in the case of an undertaking, up to 4% of the worldwide turnover, whichever is higher. The fine may be made public.*

The Lexing® network members provide a snapshot of the current state of play worldwide. The following countries have contributed to this issue: Belgium, France, Germany, Greece, Hungary, Italy, South Africa.

Lexing®

Lexing® est le premier réseau international d'avocats en droit du numérique et des technologies avancées. Créé sur une initiative d'Alain Bensoussan, Lexing® permet aux entreprises internationales de bénéficier de l'assistance d'avocats alliant la connaissance des technologies, des métiers et du droit qui leur sont applicables dans leurs pays respectifs.

Lexing® is the first international lawyers' network for digital and emerging law. Created on an initiative of Alain Bensoussan, Lexing® allows multinationals to benefit from the assistance of seasoned lawyers worldwide who each combines unique expertise in technology and industry with a thorough knowledge of law in their respective country.

https://lexing.network

VIRGINIE BENSOUSSAN-BRULÉ
Directrice du pôle Contentieux numérique du cabinet Lexing Alain Bensoussan-Avocats

Head of the Digital Litigation Division of Lexing Alain Bensoussan-Avocats

LEXING
ALAIN BENSOUSSAN AVOCATS

▪ Partout dans le monde, les autorités de contrôle effectuent des audits afin de contrôler le parfait respect, par les responsables du traitement, de la réglementation en matière de protection des données. En pratique, l'autorité compétente compare les pratiques et procédures de votre organisation avec les dispositions de la loi sur la protection des données afin de déterminer votre degré de conformité. A cette fin, l'autorité charge un de ses agents de vérifier la conformité de votre organisation en collectant les informations et documents qui pourraient être utiles. Pour de nombreux responsables du traitement, un audit peut être fortement anxiogène.

▪ Avant tout, il convient de noter que les contrôles menés par les autorités de contrôle, commissaires à l'information ou autres organismes de réglementation (1), sont à distinguer des audits effectués par votre organisation en interne, ou des audits réalisés par un tiers externe à votre organisation. Ils sont également distincts des analyses d'impact relatives à la protection des données (AIPD), des analyses d'écart, ou encore des visites de conseil réalisées à titre informel.

En quoi consiste un contrôle de conformité ?

▪ L'autorité la plus active dans le contrôle des responsables du traitement est l'autorité britannique, l'Information Commissioner's Office (ICO). Cette autorité diffuse d'ailleurs, sur son site Web, de nombreuses informations (2) ainsi qu'un guide (3) consacrés aux contrôles relatifs à la protection des données, qui donnent un bon aperçu du déroulement d'un contrôle.

▪ De manière générale, un contrôle ou un audit, qu'il soit interne ou externe, a pour but de vous aider à comprendre vos obligations en matière de protection des données et à les respecter. C'est pourquoi les rapports d'audit rédigés par les autorités de protection des données formulent des recommandations en fonction de risques constatés. Ces rapports constituent une précieuse source d'information. A cet égard, il est intéressant de souligner que l'ICO met à disposition un résumé de chacun de ses audits, d'autant plus que celui-ci consultable en ligne pendant un an après leur réalisation. Par exemple, le résumé du contrôle dont a fait l'objet de l'organisme Ormiston Academies Trust (4), suggère plusieurs pistes d'amélioration, comme la mise à jour de ses contrats de sous-traitance de données afin de les rendre pleinement conformes à l'article 28 du RGDP.

▪ Les opérations de vérifications réalisées dans le cadre de contrôles peuvent porter sur une multitude de domaines, tels que :

- la gouvernance de la protection des données,
- les structures, politiques et procédures visant à assurer le respect de la réglementation sur la protection des données,
- les processus de gestion des fichiers, automatisés et manuels, contenant des données à caractère personnel,
- les modalités de réponse aux demandes d'exercice de leurs droits par les personnes concernées,
- les mesures en place pour assurer la sécurité des données à caractère personnel stockées,

(1) Liste des autorités chargées de la protection des données, dans le monde sur le site Web de Michalsons

(2) ICO, "Audits and advisory visits: Find out about our audits and our advisory visits and how to request one", https://ico.org.uk/for-organisations/audits/

(3) ICO Guide "A guide to ICO audits", https://ico.org.uk/media/for-organisations/documents/2787/guide-to-data-protection-audits.pdf

(4) Les résultats de l'audit l'Ormiston Academies Trust quant à sa conformité en matière de protection des données effectué par l'ICO sont consultables à l'adresse : https://ico.org.uk/action-weve-taken/audits-advisory-visits-and-overview-reports/ormiston-academies-trust/

- la formation et la sensibilisation du personnel dans le domaine de la protection des données en général, et aux obligations qui leur sont imposées en particulier.

Comment se préparer à un contrôle de conformité ?

▪ Le plus important est de vous assurer de pouvoir de fournir à l'autorité de contrôle des preuves démontrant que vous prenez la protection des données au sérieux et que vous avez bien pris les mesures adaptées pour protéger les données que vous traitez. Les autorités ont besoin de preuves tangibles. Pour prouver votre conformité, vous devez donc garder une trace écrite de chacune de vos actions. Il est très difficile de remontrer le fil d'une action après coup, et il est de ce fait fortement recommandé de faire ce recensement au fur et à mesure. Si vous faîtes l'objet d'un contrôle, vous disposerez ainsi immédiatement d'une trace documentaire fiable.

▪ L'accent est généralement mis sur trois domaines :

- la sécurité des données personnelles : comment les données personnelles sont stockées et conservées en toute sécurité.
- la gestion des fichiers et des archives : comment les fichiers contenant des données personnelles sont traités (de leur collecte à leur destruction).
- la gestion des demandes relatives aux données personnelles : que ce soit les demandes présentées par les personnes concernées pour l'exercice de leurs droits, ou les demandes (régulières ou ponctuelles) de communication des données émanant d'autres organisations sont gérées.

▪ Votre organisation doit être prête à expliquer, preuves à l'appui, à l'autorité de contrôle, les procédures et systèmes spécifiques utilisés pour assurer la conformité dans ces trois domaines. Vous pouvez vous y préparer, notamment, en harmonisant le périmètre de vos audits internes avec celui des audits externes. La réalisation régulière d'audits internes, qui mettent en avant le cas échéant des recommandations et des actions correctives adaptées, permet par ailleurs d'accroitre la sensibilisation à la protection des données au sein de votre organisation.

▪ Vous pouvez également vous préparer, sur le plan juridique, en vous faisant accompagner d'un avocat spécialisé, qui vous guidera notamment dans la rédaction de la réponse à l'avis de contrôle, ainsi que sur le plan technique, en envisageant de vous équiper d'un logiciel de protection des données qui peut vous aider à prendre des mesures adéquates en temps utile et à tenir et maintenir à jour un registre des données.

Actualités : tour d'horizon des contrôles récents effectués par les autorités

▪ En Suède, l'autorité de protection des données a lancé un contrôle auprès de plus de 350 organisations issues de secteurs variés (banques, fournisseurs de télécommunications, prestataires de soins médicaux, compagnies d'assurance, syndicats, etc.) afin de vérifier l'existence d'un délégué à la protection des données. L'autorité suédoise a choisi de consacrer son premier contrôle de l'ère post-RGPD aux DPD, reconnaissant le rôle essentiel qu'ils jouent, au sein d'une organisation, en termes de conformité et de sensibilisation. Le contrôle a révélé que la majorité des entreprises contrôlées étaient en situation régulière, seules

16% d'entre elles n'ayant toujours pas, à l'époque, désigné de DPD. Si, à cette occasion, l'autorité suédoise a prononcé quelques rappels à l'ordre et mises en demeure sans les assortir de sanction financière, sa présidente Lena Lindgren Schelin a précisé que les contrevenants seront à l'avenir passibles d'une amende.

▪ En Allemagne, l'autorité de protection des données de l'Etat de Bavière a mené un contrôle portant sur l'utilisation de cookies et autres traceurs par les principaux sites Web bavarois. En effet, conformément à la position adoptée le 26 avril 2018 par la Conférence des autorités allemandes de protection des données, l'utilisation de cookies nécessite le consentement explicite des internautes. Or, les investigations de l'autorité ont révélé qu'aucun des 40 sites Web n'était en conformité sur ce point.

▪ Au Royaume-Uni, l'autorité de contrôle a réalisé 55 audits à ce jour. Les contrôles formels et informels mis en œuvre par l'ICO sont recensés sur son site Web (5). A l'issue de ses opérations de contrôle, l'ICO attribue une note indicatrice du niveau de conformité. Le système de notation de l'ICO comprend quatre niveaux, en fonction du niveau de conformité présentés par les éléments audités au regard de la réglementation en matière de protection des données : élevé, raisonnable, limité ou très limité. Par exemple, l'organisme en charge du système de santé pour l'Angleterre, NHS England (6), a fait l'objet d'un audit axé sur la gouvernance et la responsabilisation, aux termes duquel il s'est vu attribué un niveau de conformité « raisonnable » et préconisé d'améliorer davantage sa politique d'audit.

▪ Plus tôt cette année, l'ICO a annoncé envisager d'infliger de lourdes amendes à deux entreprises pour violation du RGPD. La compagnie aérienne British Airways pourrait écoper d'une amende de plus de 183 millions de livres (200 millions d'euros), tandis que le groupe d'hôtellerie Marriott International se verrait condamné à une amende de près de 100 millions de livres (110 millions d'euros). Si ces sanctions pécuniaires ne sont pas encore confirmées, les deux entreprises contrevenantes ayant la possibilité de plaider leur cause avant la prise de décision finale du gendarme britannique de protection des données. (7), ces décisions témoignent de l'intensification des mesures correctrices adoptées par l'ICO (les amendes similaires imposées avant l'entrée en vigueur du RGPD tournaient autour des 500.000 £, soit environ 583.000 €) et préfigurent l'augmentation croissante des contrôles par l'ensemble des autorités de protection de données dans le monde.

(5) Page Web de l'ICO « Audits, advisory visits and overview reports» : https://ico.org.uk/action-weve-taken/audits-advisory-visits-and-overview-reports/

(6) Les résultats de l'audit de NHS England quant à sa conformité en matière de protection des données effectué par l'ICO sont consultables à l'adresse *:* https://ico.org.uk/action-weve-taken/audits-advisory- visits-and-overview- reports/nhs-england/

(7) "Is the ICO being too harsh with its GDPR fines?", Michalsons, https://www.michalsons.com/blog/is-the-ico-being-too-harsh-with-its-gdpr-fines/39641

JOHN GILES

south-africa@lexing.network

▪ *Data protection authorities around the world have started to do a data protection audit (or GDPR audit) on controllers to check that they comply with data protection law. Essentially, the authority compares your organisation to a data protection law that it must comply with and determines the degree to which your organisation complies. A compliance audit involves an auditor from an authority verifying your organisation's compliance with the law by gathering evidence. For many controllers, this is a very scary prospect.*

▪ *Please note that this article is specifically about an authority, commissioner or regulator (1) conducting an audit. It is not about an internal audit or other external third-party is doing an audit on you. It is also not about a privacy impact assessment (PIA) or a data protection gap analysis. This article is also not about a GDPR data audit, which is something different. An audit is also something different to an advisory visit.*

What is involved in a data protection audit?

▪ *The authority who is most active in auditing controllers is the Information Commissioners Office (ICO) in the United Kingdom. They have also given us information (2) and a guide (3) to ICO data protection audits. This material is very useful for giving you an idea of what would be involved.*

▪ *An audit, both internal and external, should be aimed at helping you understand your data protection obligations as well as at meeting them. Data protection authorities, such as the ICO, provide a risk focused report with recommendations after they've assessed the extent to which you comply with the relevant data protection law. The ICO also publishes an executive summary on their website for a year after the audit. For example, there is an executive summary of the recent Ormiston Academies Trust audit (4) that notes areas of improvement such as updating their contracts with data processors to be fully compliant with Article 28 of the GDPR.*

▪ *An audit may look at a number of areas relevant to your organisation. Some examples include:*

- *data protection governance,*
- *the structures, policies and procedures to ensure compliance with data protection legislation,*
- *the processes for managing both electronic and manual records containing personal data,*
- *the processes for responding to any request for personal data,*
- *the measures in place to ensure the security of personal data you store, and*
- *the provision of staff data protection training and staff awareness of data protection requirements.*

How to prepare for a GDPR audit

▪ *Essentially you want to be in a position to provide an authority with tangible evidence that you take data protection seriously and that you have correctly taken action to protect personal data. Authorities like evidence. So you need to start creating a paper trail of all the actions you have taken over time. This is very hard*

(1) List of data protection authorities, Information commissioners or regulators (DPAs) on Michalsons' website

(2) ICO, "Audits and advisory visits: Find out about our audits and our advisory visits and how to request one", https://ico.org.uk/for-organisations/audits/

(3) ICO Guide "A guide to ICO audits": https://ico.org.uk/media/for-organisations/documents/2787/guide-to-data-protection-audits.pdf

(4) The ICO has carried out a data protection audit of Ormiston Academies Trust with its consent: https://ico.org.uk/action-weve-taken/audits-advisory-visits-and-overview-reports/ormiston-academies- trust/

to recreate when you're being audited and is much easier to do over a period of time when you are actually taking the action.

- *Audits look at three main areas:*
  - *Security of personal data – how personal data is stored and kept secure.*
  - *Records management – how records containing personal data are processed, from collection to destruction.*
  - *Requests for personal data – how you handle individuals' requests for copies of their personal data and how you manage routine and one off disclosures to other organisations.*

- *Your organisation should be prepared to show a data protection authority the specific processes and facilities employed to meet compliance in these areas. You can prepare by aligning your internal audit with an external one. By running regular internal audits that include recommendations and actionable tasks you'll increase data protection awareness across your organisation.*

- *You can prepare by finding data protection software that can help you take action and produce a record of what is being done.*

Recent high profile audits by authorities

- *Recently, the Swedish Data Protection Authority has performed an audit of over 350 organisations on whether they had yet to appoint a data protection officer. The audit included, amongst others, banks, telecom providers, medical care providers, insurance companies and trade unions. This is their first GDPR audit and they chose to audit the presence of appointed Data Protection Officers because the role is critical to raise data protection awareness within an organisation as well as to compliance. The audit shows, among other things, that most companies have. Only 16% of the audited companies still need to appoint a Data Protection Officer. The Swedish DPA issued reprimands and orders to comply but no fines. Inspector General Lena Lindgren Schelin has said fines will be on the table in the future for continued non-compliance.*

- *The Bavarian Data Protection Authority audited major Bavarian websites for their use of tracking tools, specifically looking at the use of cookies. According to the Conference of German Data Protection Authorities' position paper on 26 April 2018, the use of cookies requires opt-in consent. The authority found none of the 40 websites they audited to be compliant.*

- *The ICO has conducted 55 audits so far. They report their audits and advisory visits (5) on their website. Recently they conducted an audit of the NHS England (6) focusing on governance and accountability. Their rating system consists of four categories, High, Reasonable, Limited or Very Limited. The NHSE were given a 'Reasonable' assurance rating and were advised to revise their information management audit framework.*

- *Earlier this year, the ICO proposed fining British Airways more than £183 million and Marriott International almost £100 million. Whilst these are only proposed fines and so are likely to be reduced, (7) this is an indication that data protection authorities are intensifying their activities as similar fines in the pre-GDPR era were around £500 000. This might also be an indicator that authorities will conduct a greater number of audits in future.*

(5) ICO webpage "Audits, advisory visits and overview reports": https://ico.org.uk/action-weve-taken/audits-advisory-visits-and-overview-reports/

(6) The ICO has carried out a data protection audit of NHS England with its consent.: https://ico.org.uk/action-weve-taken/audits-advisory-visits-and-overview-reports/nhs-england/

(7) "Is the ICO being too harsh with its GDPR fines?", Michalsons, https://www.michalsons.com/blog/is-the-ico-being-too-harsh-with-its-gdpr-fines/39641

JOHN GILES

south-africa@lexing.network

▪ Depuis l'entrée en vigueur du RGPD, l'actualité dans le domaine de la protection des données a été riche. Tandis que les entreprises ont modernisé leurs procédures et systèmes internes de protection des données, les autorités chargées de la protection des données ont, quant à elles, renforcé leur personnel et leur organisation. De nombreux contrôles et audits ont été menés dans les entreprises et plusieurs amendes ont déjà été infligées.

▪ En Allemagne, Etat fédéral, les autorités de protection des données des différents Länder fixent chacune leurs priorités en matière de contrôle. En janvier 2019, par exemple, l'autorité de contrôle de la protection des données pour l'Etat de Bavière s'est concentrée sur l'utilisation d'outils de suivi en ligne. A l'occasion de la Journée pour un internet plus sûr, 40 sites web d'entreprises bavaroises ont ainsi été examinés à la loupe afin d'identifier l'existence d'outils de suivi et d'analyse, la base juridique sur laquelle repose leur utilisation, et le respect du cadre légal en matière de protection des données. Cette enquête a révélé qu'aucun des 40 sites audités n'avait obtenu le consentement effectif des visiteurs du site pour l'usage de ces outils. (1)

(1) Communiqué de presse, 5-11-2019, accessible à l'adresse suivante : https://www.lda.bayern.de/media/pm2019_3_de.pdf

▪ De son côté, l'autorité de protection des données de l'Etat de Basse-Saxe a adopté une démarche différente. Elle a choisi de procéder à un état des lieux en imposant à 50 grandes et moyennes entreprises de compléter un questionnaire détaillé. Si la publication de l'analyse des réponses à ce questionnaire se fait toujours attendre, le commissaire à la protection des données du Land de Basse- Saxe a néanmoins annoncé, lors d'une conférence, que les plus importants écarts de conformité identifiés concernaient les analyses d'impact relatives à la protection des données (AIPD) et les mesures techniques et organisationnelles, et ce alors que le RGPD a accru l'obligation pour les organisations d'assurer la sécurité des données à caractère personnel qu'elles traitent, compte tenu de l'état des connaissances. La question de la sécurité continuera sans nul doute de faire l'objet de vérifications de plus en plus nombreuses à l'avenir. L'autorité bas- saxonne a enfin clairement annoncé qu'elle comptait infliger des amendes pour les infractions constatées au cours de cette enquête.

▪ La diffusion publique par l'autorité de Basse-Saxe de son questionnaire est salutaire, en ce qu'elle permet à toutes les entreprises d'autoévaluer, en amont, leur conformité aux exigences du RGPD ainsi que l'adéquation de leur fonctionnement aux critères pris en compte par l'autorité. Le questionnaire s'articule autour des dix thèmes suivants : mesures de préparation au RGPD, registres des activités de traitement, bases juridiques du traitement, protection des droits des personnes concernées, protection technique des données, AIPD, sous-traitance, délégué à la protection des données, obligations de notification, et documentation. Ces thèmes se déclinent ensuite en sous-thèmes, plus détaillés. (2)

(2) https://lfd.niedersachsen.de/startseite/datenschutzreform/ds_gvo/kriterien-querschnittspruefung-179455.html

▪ Dans le même ordre d'idée, l'autorité de contrôle bavaroise a également diffusé son propre questionnaire. Celui-ci, intitulé « audit de mise en œuvre du RGPD », s'adresse explicitement aux petites et moyennes entreprises. Contrairement au

questionnaire de l'autorité bas-saxonne qui est assez exhaustif, le questionnaire bavarois est, lui, beaucoup plus succinct (il ne comporte que 20 questions au total) et se présente sous forme de cases à cocher associées à des réponses préformulées, par lesquelles les entreprises indiquent l'état d'avancement de leur mise en œuvre du RGPD. Le questionnaire doit être renvoyé complété et accompagné, le cas échant, d'une copie de tous documents pertinents, tels que les concepts de protection des données ou les formulaires de consentement utilisés par l'organisme. (3). Ces différents éléments peuvent également constituer une liste de contrôle lors d'un examen non officiel d'une autorité.

(3) https://www.lda.bayern.de/media/pruefungen/201811_kmu_fragebogen.pdf

▪ Dans l'ensemble, il apparaît que les autorités procèdent de plus en plus souvent à des contrôles, et tout indique que cette tendance va s'inscrire dans la durée. (4) Comme l'ont montré les initiatives décrites plus haut, les contrôles ne sont plus déclenchés uniquement par des réclamations déposées par des personnes concernées. Ils peuvent également avoir lieu à l'initiative des autorités elles- mêmes. Un des enseignements à tirer des décisions déjà prononcées est qu'il est essentiel de coopérer avec les autorités afin d'espérer obtenir une réduction de la sanction qui pourrait être éventuellement décrétée aux termes de la procédure d'audit.

(4) Une liste des contrôles en cours en Bavière peut être consultée à l'adresse suivante : https://www.lda.bayern.de/d e/kontrollen.html

▪ La première grosse amende infligée en Allemagne sous l'empire du RGPD fut prononcé à l'encontre d'un réseau social, pour mesures de protection insuffisantes, les données de ses utilisateurs ayant fuité sur internet à la suite d'une cyberattaque dont il a été victime. Grâce à sa coopération exemplaire saluée par l'autorité de protection des données du Bade-Wurtemberg, le réseau social a pu éviter une amende salée et n'être condamné qu'à « seulement » 20.000 euros.
(5) Dans une autre affaire, une entreprise qui avait, pour des raisons financières, renoncé à la conclusion d'un contrat de sous-traitance en bonne et due forme, en dépit de la recommandation expresse de l'autorité contrôle de Hambourg, a été punie d'une amende de 5.000 euros. (6)

(5) Communiqué de presse, 22-11-2018, accessible à l'adresse suivante : https://www.baden-wuerttemberg.datenschutz.de/lfdi-baden-wuerttemberg-verhaengt-sein-erstes-bussgeld-in-deutschland-nach-der-ds-gvo/

(6)(6) https://www.heise.de/newsticker/meldung/DSGVO-5000- Euro-Bussgeld-fuer-fehlenden-Auftragsverarbeitungsvertrag-4282737.html.

▪ A l'évidence, le mot d'ordre pour une bonne préparation aux contrôles de conformité est la prise en compte des positions et avis adoptés par les autorités de protection des données, que ceux-ci soient diffusés soit directement à votre organisme sous la forme d'avis individuel personnalisés, soit à l'ensemble du public sous la forme de recommandations générales pour la bonne application des règles informatique et libertés.

SUSANNE KLEIN

germany@lexing.network

▪ *A lot has happened since the GDPR came into force. Not only the companies have upgraded their data protection equipment, but also the data protection authorities have strengthened their personnel and organisation. As a result, initial audits and inspections have taken place in companies and various fines have already been imposed.*

▪ *The main focus of the previous audits was set differently by the data protection authorities of the federal states. In January 2019, for example, the Bavarian data protection supervisory authority specifically examined the use of online tracking tools in compliance with data protection regulations. For this purpose, 40 websites of Bavarian companies were examined on the occasion of Safer Internet Day to determine whether they use tracking and analysis tools, on what legal basis this is done and whether this has been implemented in compliance with data protection regulations. The result was that none of these 40 websites obtained the effective consent of the website visitors. (1)*

(1) Press release from 5 February 2019: https://www.lda.bayern.de/media/pm2019_3_de.pdf

▪ *The data protection authority of Lower Saxony, however, took a different approach. It sent an extensive questionnaire to 50 large and medium-sized companies in its area of responsibility, which they had to complete and return. The official publication of the results of this survey is still pending. However, the State Data Protection Commissioner of Lower Saxony announced at a conference that the survey focused on the areas of data protection impact assessments as well as on the technical and organisational measures taken by companies, and that the biggest deficits identified were also in these areas. It was clarified that the GDPR places a greater obligation on companies to ensure the security of personal data by means of an appropriate state of the art. This will continue to be the subject of more and more audits in the future. In addition, the authority has announced that it will also initiate fine proceedings in respect of the infringements identified in the course of the survey.*

▪ *However, it is very helpful that the Lower Saxony authority has published its questionnaire. This enables companies themselves to proactively check whether they already meet the GDPR's requirements and are thus set up in a way that conforms to the authority's data protection requirements. The checklist comprises the following ten subject areas: Preparation for the GDPR, records of processing activities, legal bases for processing, protection of data subjects' rights, technical data protection, data protection impact assessment, order processing, data protection officer, notification obligations and documentation. Detailed sub-questions can be found in each area. (2)*

(2) https://lfd.niedersachsen.de/startseite/datenschutzreform/ds_gvo/kriterien-querschnittspruefung-179455.html

▪ *The Bavarian State Office for Data Protection Supervision, which has also made a questionnaire available for download, proceeded in a similar manner. This questionnaire for the "GDPR implementation audit" is expressly addressed to small and medium-sized enterprises, which were the focus of the authority's attention here. In contrast to the extensive questionnaire of the Lower Saxony Authority, this survey is considerably shorter because there are only 20 questions in total and the companies have the opportunity to indicate the status of their implementation of*

the GDPR by ticking pre-formulated answers. In addition, any existing documents, such as data protection concepts or declarations of consent, should also be sent for examination. (3) This list of questions can also be used as the basis for an authority's own internal review without an official review.

▪ *Overall, it is becoming apparent that the authorities are already increasingly carrying out audits and will continue to do so. (4) As the described procedures show, audits are no longer only carried out on the basis of complaints from data subjects, but also on the initiative of the authorities themselves. The fines already published show that it is always advisable to cooperate with the authorities, which can directly reduce the fine.*

▪ *The first higher fine in Germany under the GDPR was imposed on a social network because it had not sufficiently protected the access data of its users and they were published unprotected on the Internet due to a hacker attack. A fine of "only" EUR 20,000 was imposed for these offences, whereby the data protection authority of Baden Württemberg expressly clarified that the exemplary cooperation of those responsible with the authority in clarifying the incident had led to a significant reduction in the fine. (5) On the other hand, a fine of EUR 5 000 was imposed by the Hamburg supervisory authority for lack of a contract for order processing because, contrary to the express recommendation of the authority, the undertaking concerned had refrained for cost reasons from taking care of such a contract. (6)*

▪ *All this shows that it is advisable to take into account the advice of the data protection supervisory authorities, whether this is given in a specific individual case or as general assistance for the implementation of the GDPR.*

(3) https://www.lda.bayern.de/media/pruefungen/201811_kmu_fragebogen.pdf

(4) A list of current investigations in Bavaria can be found here: https://www.lda.bayern.de/de/kontrollen.html

(5) Press release from 22 November 2018: https://www.baden-wuerttemberg.datenschutz.de/lfdi-baden-wuerttemberg-verhaengt-sein-erstes-bussgeld-in-deutschland-nach-der-ds-gvo/

(6)(6) https://www.heise.de/newsticker/meldung/DSGVO-5000-Euro-Bussgeld-fuer-fehlenden-Auftragsverarbeitungsvertrag-4282737.html.

SUSANNE KLEIN

germany@lexing.network

REFERENCES

Quelle méthode utiliser ?

▪ L'Autorité de protection des données belge recommande (1) que le responsable du traitement s'appuie sur les normes internationales de gestion des risques existantes, telles que celles élaborées par l'Organisation internationale de normalisation (ISO) ou les codes de conduite élaborés ou adoptés au niveau européen.

▪ Concernant les analyses d'impact, le responsable du traitement est en principe libre de choisir la méthode qu'il souhaite utiliser, à condition qu'elle réponde à un certain nombre de caractéristiques minimales de confidentialité et d'objectivité, qu'elle prenne en compte les éléments minimaux prescrits par le RGPD et qu'elle soit adaptée aux besoins et au contexte de l'entreprise.

▪ Quelle que soit la méthode choisie par le responsable du traitement, la Commission de la protection de la vie privée considère comme essentiel que le responsable du traitement indique explicitement quelle méthode a été choisie et qu'elle soit appliquée de manière cohérente tout au long du processus.

Sites web

▪ Les responsables du traitement peuvent utiliser l'outil gratuit développé par le Contrôleur européen de la protection des données (2) pour automatiser les contrôles relatifs à la protection des données personnelles sur les sites web.

▪ L'outil recense les différents traitements des données personnelles, tels que les cookies ou les demandes adressées à des tiers, selon des paramètres configurés avant l'inspection.

▪ Le résultat permet aux contrôleurs de site Web de mieux comprendre quelles informations sont transférées et stockées lors d'une visite d'un site web.

Subsides

▪ Les acteurs économiques basés à Bruxelles et en Wallonie (3) peuvent demander des subsides pour les audits de cybersécurité, s'élevant respectivement de 50% et 75% du coût de l'audit.

▪ A notre connaissance, aucune aide équivalente n'est offerte aux entreprises basées en Flandre.

Quels sont les audits pratiqués par l'Autorité de protection des données sur les 6 derniers mois ?

▪ Comme il a fallu près d'un an pour constituer le DPA belge, aucune enquête proactive n'a encore eu lieu.

Jusqu'à ce jour, la Chambre Contentieuse n'a rendu de décisions qu'à la suite de plaintes précises (4), et non à l'issue d'une enquête exhaustive.

(1) Recommandation n°01/2018 du 28 février 2018 : https://www.gegevensbescherming sautoriteit.be/sites/privacycommission/files/documents/recommandation_01_2018_0.pdf

(2) EDPS Website Evidence Collector : https://edps.europa.eu/press-publications/edps-inspection-software_en

(3) Subsides : http://werk- economie-emploi.brussels/fr_FR/prime-consultance
Wallonie : https://www.cheques-entreprises.be/cheques/cybers ecurite/

(4) Décisions de la Chambre Contentieuse de l'Autorité de protection des données belge : https://www.autoriteprotectio ndonnees.be/decisions-de-la- chambre-contentieuse

FANNY CONTON

belgium@lexing.network

Which method to use?

- *The Belgian DPA recommends (1) that the controller should rely on existing international risk management standards, such as those developed by the International Organisation for Standardisation (ISO) or codes of conduct developed or agreed at European level.*
- *Regarding PIA, the DPA stresses the fact that the controller is free to choose the method he or she wishes to use, provided that it meets a number of minimum characteristics of confidentiality and objectivity and takes into account the minimum elements prescribed by the GDPR and is adapted to the needs and context of the company.*
- *Whatever the method finally chosen by the controller, the Privacy Commission considers it essential that the controller should explicitly indicate which method has been chosen and that it should be applied consistently throughout the process.*

Websites

- *Data controllers can use the free tool developed by the European Data Protection* Supervisor (2) to *automate personal data protection controls on websites.*
- *The tool identifies the different data processing, such as cookies or requests to third parties, according to parameters configured before the inspection.*
- *The result allows website controllers to better understand what information is transferred and stored when visiting a website.*

Subsidies

- *Economic actors based in Brussels and Wallonia (3) can ask for public subsidies for cybersecurity audits, respectively from 50% and 75 % of the cost of the audit.*
- *To our knowledge, no equivalent subsidies are offered to Flemish based companies.*

Where are we since the last 6 months in terms of DPA audits?

- *Since it took nearly a year to constitute the Belgian DPA, no proactive investigation has taken place yet.*
- *To date, the Chamber (4) has only rendered decisions following specific complaints, and not after an exhaustive investigation.*

REFERENCES

(1) Belgian DPA Recommendation n° 01/2018 (February 28th 2018): https://www.gegevensbescher mingsautoriteit.be/sites/privac ycommission/files/documents/ recommandation_01_2018_0.pdf

(2) EDPS Website Evidence Collector: https://edps.europa.eu/press-publications/edps-inspection-software_en

(3) Subsidies:
In Brussels: http://werk- economie-emploi.brussels/fr_FR/prime-consultance
In Wallonia: https://www.cheques-entreprises.be/cheques/cybers ecurite/

(4) DPA Dispute Chamber decisions: https://www.autoriteprotecti o ndonnees.be/decisions-de-la- chambre-contentieuse

FANNY CONTON

belgium@lexing.network

▪ Le contrôle peut porter sur tout traitement de données à caractère personnel mis en œuvre, en tout ou partie, sur le territoire français, même lorsque le responsable du traitement est établi sur le territoire d'un autre Etat membre de l'Union européenne.

▪ Le responsable du traitement est le représentant légal de l'entreprise alors que le responsable des lieux est la personne habilitée, au sein des locaux contrôlés, à représenter l'organisme responsable du traitement, par exemple du fait d'une délégation de pouvoir.

▪ C'est la Cnil qui a l'initiative du contrôle, sur décision de son Président après proposition des services de contrôle, qui peut faire suite à notamment à :

- une plainte ou une réclamation d'un tiers ;
- la demande d'une autorité en charge de la protection des données européenne ;
- la demande d'une autorité en charge de la protection des données non européenne ;
- lorsque l'organisme est inscrit dans le programme annuel thématique des contrôles de la Cnil.

▪ L'objectif de la Cnil c'est de vérifier que la réglementation est respectée par les organismes contrôlés.

▪ Il existe quatre types de contrôle :

- le contrôle sur place ;
- le contrôle sur pièces ;
- l'audition sur convocation ;
- le contrôle en ligne qui permet à la Cnil de procéder à des constatations en ligne depuis ses locaux, hors la présence du responsable du traitement. Ce contrôle porte sur les données librement accessibles ou rendues accessibles en ligne, y compris par imprudence, négligence ou par le fait d'un tiers, et peut-être complémentaire à un autre type de contrôle.

▪ La Cnil doit informer de :

- l'objet du contrôle ;
- l'identité et la qualité des personnes contrôlées ;
- le cas échéant, le droit d'opposition.

▪ La Cnil doit donner ces informations aux personnes suivantes notamment :

- le procureur de la République
- le responsable du traitement
  - lorsque le contrôle se déroule sur place, le responsable du traitement est informé au début du contrôle. L'information préalable du
    responsable du traitement est une décision prise en opportunité par la Cnil ;

- lorsque le contrôle se déroule sur audition, le responsable du traitement doit être convoqué au moins 8 jours avant la date du contrôle ;
- lorsque le contrôle est effectué à la demande d'une autorité de contrôle d'un Etat membre de l'Union européenne, le responsable du traitement doit en être informé ainsi que du fait que les informations recueillies ou détenus par la Cnil sont susceptibles d'être communiquées à cette autorité.

▪ Il peut être demandé au responsable du traitement de préparer tous documents de nature à faciliter son déroulement.

▪ Le responsable des lieux est informé de son droit à s'opposer au contrôle. S'il exerce ce droit :

- les motifs de son opposition sont portés au procès-verbal dressé par les agents de la Cnil ;
- les opérations de contrôle ne peuvent intervenir qu'après autorisation du juge des libertés et de la détention.

▪ Le délit d'entrave à l'action de la Cnil est puni d'un an d'emprisonnement et de 15 000 euros d'amende. Ce délit est constitué par :

- Le refus de se soumettre à l'exercice de vérifications malgré l'autorisation du juge des libertés et de la détention ;
- le refus de communiquer aux agents de la Cnil les renseignements et documents utiles à leur mission en les dissimulant ou en les faisant disparaître ;
- la communication d'informations non conformes au contenu des enregistrements tel qu'il était au moment où la demande a été formulée ou qui ne présentent pas ce contenu sous une forme directement accessible.

▪ Les agents de la Cnil peuvent procéder à des opérations de contrôle de traitement dans les locaux du responsable du traitement entre 6 heures et 21 heures.

▪ Ils ont accès aux lieux, locaux, enceintes, installations ou établissements servant à la mise en œuvre d'un traitement de données à caractère personnel et à usage professionnel, à l'exclusion des parties de ceux-ci affectées au domicile privé.

▪ Une mission de contrôle vise prioritairement à obtenir copie du maximum d'informations, techniques et juridiques, pour apprécier les conditions dans lesquelles sont mis en œuvre des traitements de données à caractère personnel.

▪ Dans le cadre des opérations de contrôle, les agents de la Cnil sont autorisés à :

- obtenir communication et copie de tout document, quel qu'en soit le support, leur permettant d'apprécier les conditions dans lesquelles des traitements de données à caractère personnel sont mis en œuvre ;
- accéder aux programmes informatiques et aux données ;
- demander la transcription de tout document directement utilisable pour les besoins du contrôle ;
- recueillir tout renseignement technique ou juridique ou toute justification utile à l'accomplissement de leur mission.

▪ Le procès-verbal de constatation est établi sur la base des éléments recueillis lors du contrôle et contient notamment :

- l'objet de la mission de contrôle ;
- la nature du contrôle ;
- le jour et l'heure des opérations de contrôle ;
- le lieu du contrôle ;
- les agents de la Cnil présents lors du contrôle ;
- les personnes rencontrées ;
- les contrôles effectués ;
- les éventuelles difficultés rencontrées ;
- le cas échéant, l'opposition au contrôle du responsable des lieux.

▪ En annexe du procès-verbal, figure l'inventaire des pièces et documents dont les agents de la Cnil ont pris copie.

▪ Le responsable des lieux peut émettre des réserves et des commentaires sur le procès-verbal.

▪ Le procès-verbal est signé par agents de la Cnil et par le responsable des lieux et notifié au responsable du traitement.

▪ A la suite du contrôle, la Cnil examine les documents dont copie a été réalisée pour apprécier si les dispositions de la loi Informatique et libertés ont été respectées.

▪ Lorsque l'examen n'appelle pas d'observations particulières, un courrier est adressé par le Président de la Cnil au responsable du traitement. Ce courrier peut contenir des recommandations telles que les modifications des durées de conservation ou des mesures de sécurité complémentaires.

▪ Lorsque l'examen fait ressortir des manquements sérieux, le dossier est transmis à la formation contentieuse de la Cnil, transmission non exclusive d'une dénonciation auprès du procureur de la République.

▪ Les principaux conseils que l'on peut donner, à la fois en prévision et lors d'un contrôle sur place de la Cnil sont les suivants :

- anticiper un contrôle en vérifiant la bonne application de la réglementation sur la protection des données personnelles notamment en termes de sécurité, d'information de personnes et de modalité de collecte des données ;
- mettre en place une procédure interne applicable en cas de contrôle de la Cnil, afin que ce dernier se déroule dans les meilleurs conditions possibles tant pour l'organisme contrôlé que pour les agents de la Cnil ;
- former et informer son personnel.

VIRGINIE BENSOUSSAN-BRULÉ

france@lexing.network

▪ *A GDPR audit carried by the French data protection authority (CNIL) may cover any processing of personal data carried out, in whole or in part, on the French territory, even where the controller is established in the territory of another Member State of the European Union.*

▪ *The controller is the legal representative of the organisation and may be different from the person in charge of the audited premises, who should be entitled to represent the controller, for example by virtue of a delegation of power.*

▪ *Audits are initiated by the CNIL, upon decision of its President and after proposal from its audit department, which may notably act on:*

- *a complaint or claim from a third party;*
- *at the request of a EU data protection authority;*
- *at the request of a non-EU data protection authority;*
- *when the organisation is included in the CNIL's annual audit programme.*

▪ *The objective of the CNIL is to verify that the audited organisation complies with the applicable laws and regulations.*

▪ *There are four types of audits:*

- *(i) On-site audits;*
- *(ii) Desk audits;*
- *(iii) Audits during a hearing (hearing on notice);*
- *(v) Online audits, where the CNIL can investigate online from its premises, without the presence of the controller. Online audits cover data that are freely accessible or made accessible online, including through carelessness, negligence or the actions of a third party, and may be conducted in combination with another type of audit.*

▪ *The CNIL must provide information about:*

- *the subject matter of the audit;*
- *the identity and title of the persons to be audited;*
- *where applicable, the right to object to the audit.*

▪ *The above information should be provided by the CNIL to the following persons:*

- *the public prosecutor*
- *the controller*
  - *when the audit is carried out onsite, information is provided at the beginning of the onsite audit. The CNIL may decide at its sole discretion to inform to the controller in advance;*
  - *when the audit is carried out during a hearing, the controller must be summoned at least 8 days before the date of the audit;*
  - *when the audit is carried out at the request of a supervisory authority of a EU Member State, the controller must be informed thereof and of the fact that the information collected or held by the CNIL may be communicated to that authority.*

▪ *The controller may be asked to prepare any documents likely to facilitate the audit.*

▪ *The person in charge of the premises is informed of their right to object to the audit. If that person objects to the audit:*

- *the reasons for their objection will be recorded in the report drawn up by the CNIL agents;*
- *the audit operations may only be carried out after authorisation by the liberty and custody judge.*

▪ *Obstructing the CNIL's action is an offence punished by one year's imprisonment and a fine of 15,000 euros. This offence consists in:*

- *refusing to submit to the audit despite the authorisation given by the liberty and custody judge;*
- *refusing to provide the CNIL agents with the information and documents required for the performance of their tasks by concealing such information and documents or making them disappear;*
- *communicating information whose content is different from the one existing before the request was made or Is not in a directly accessible form.*

▪ *CNIL agents are entitled to audit processing on the premises of the controller between 6 a.m. and 9 p.m.*

▪ *They may access places, premises, surroundings, facilities or establishments where personal data are processed and which are used for professional purposes, with the exception of the parts of those places, premises, surroundings, equipment or buildings which are used for private purposes.*

▪ *The primary aim of an audit is to obtain copies of as much technical and legal information as possible in order to assess the conditions in which personal data are processed.*

▪ *To this end, the CNIL agents are authorised:*

- *to obtain communication and copies of any document, whatever the medium, enabling them to assess the conditions under personal data are processed.*
- *to access electronic data processing programmes and data;*
- *to ask for the transcription of such programmes and data into directly usable documents for the purposes of the audit;*
- *to collect any technical or legal information or proof necessary for the performance of their tasks.*

▪ *At the end of the audit, a report is drawn up on the basis of the information gathered during the audit. The audit report will include information such as:*

- *the subject matter of the audit;*
- *the nature of the control;*
- *the date and time of the audit;*
- *the location where the audit took place;*
- *the CNIL agents who were present during the audit;*
- *the individuals met;*
- *the controls carried out;*

- *where applicable, the difficulties encountered;*
- *where applicable, the fact that the person in charge of the premises has objected to the audit.*

▪ *A list of the documents and materials copied by the CNIL agents should be attached to the report.*

▪ *The person in charge of the premises may ask to include any reservations and comments they may have in the report.*

▪ *The report must be signed by the CNIL agents and by the person in charge of the premises; it is notified to the controller.*

▪ *After the audit, the CNIL will review the documents copied and assess whether the provisions of the French Data Protection Act have been complied with.*

▪ *When the review does not call for any specific comments, a letter will be sent by the President of the CNIL to the controller. This letter may contain recommendations, such as changing data retention periods or introducing additional security measures.*

▪ *When the review reveals serious infringements, the file is escalated to the CNIL's sanctions committee, and may be transmitted to the public prosecutor.*

▪ *Tips and advice before, during and after a CNIL audit:*

- *Anticipate the audit by verifying your proper application of the applicable laws and regulations on the protection of personal data, with particular focus on data security, data subject information, and data collection methods;*
- *Proactively set up an internal procedure applicable in the event of an audit of the CNIL, so that the audit may take place in the best possible conditions for both your organisation and the CNIL agents;*
- *Train, inform and raise the awareness of your staff.*

VIRGINIE BENSOUSSAN-BRULÉ

france@lexing.network

Prendre acte de la fin de la période de grâce

▪ Près de 14 mois après le 25 mai 2018, date d'application du Règlement général sur la protection des données (UE) 2016/679 (RGPD), l'autorité grecque de protection des données a publié, sur son site Web, la première décision dans laquelle elle exerce les mesures correctrices qui lui sont désormais conférés par le RGPD. Par cette décision 26/2019 daté du 30 juillet 2019 (1), elle inflige une amende de 150.000 euros à la société PricewaterhouseCoopers Business Solutions
S.A. (PwC BS) pour violation des principes de licéité (base juridique inappropriée pour le traitement des données de ses employés) et de responsabilité. Par ailleurs, l'autorité s'est également engagée dans un programme de contrôle de conformité au RGPD mené auprès d'organismes aussi bien du secteur privé (et plus particulièrement dans les domaines de l'assurance, de la finance et du commerce électronique) que du secteur public. Elle a également adressé plusieurs avertissements à des responsables du traitement, les alertant sur le fait que les opérations de traitement envisagées étaient susceptibles de violer les dispositions du RGPD.

(1) Résumé officiel de la décision 26/2019 disponible (en anglais) à l'adresse : https://www.dpa.gr/pls/portal/docs/PAGE/APDPX/ENGLISH_INDEX/DECISIONS/SUMMARY%20OF%20DECISION%2026_2019%20(EN).PDF

S'assurer de la licéité du traitement

▪ L'affaire PwC constitue un précédent utile sur lequel les responsables du traitement et les sous-traitants grecs peuvent s'appuyer pour se préparer au mieux aux contrôles de l'autorité. Notamment, dans sa décision, l'autorité a clairement et expressément indiqué que lorsque le responsable du traitement a des doutes quant à la licéité du traitement, il doit absolument s'abstenir de procéder à toute opération de traitement jusqu'à ce que les mesures prises aient permis de les dissiper.

Documenter la conformité

▪ Il ressort en outre de cette décision que le respect du principe de responsabilité impose de constituer et de regrouper la documentation nécessaire à chaque étape du traitement. En effet, l'autorité hellénique a « attach[é] une importance particulière au fait que le responsable du traitement n'a été en mesure de fournir aucune preuve permettant de justifier le choix de la base juridique qu'il considérait appropriée ».

Prendre des mesures correctives

▪ En cas de constat de non-conformité, des mesures correctives doivent être prises dès que possible, et idéalement avant la fin du contrôle conduit par l'autorité. De fait, en l'espèce, pour décider de la sanction à imposer, l'autorité a tenu dûment compte du fait que le responsable du traitement n'avait pas pris les mesures correctives pourtant annoncés à l'autorité.

Se faire accompagner par des professionnels

▪ Compte tenu des enjeux, il essentiel de faire appel à des experts qui vous accompagneront dans la mise en œuvre de votre stratégie de conformité au RGPD, ainsi qu'en cas de contrôles réalisés par l'autorité. Ce soutien pèsera dans la balance lorsqu'il s'agira de déterminer la probabilité et la nature des sanctions encourues en cas de non-conformité.

GEORGE A. BALLAS
&
THEODORE KONSTANTAKOPOULOS

greece@lexing.network

Grace period is over

▪ *Almost 14 months after May 25, 2018, when the General Data Protection Regulation (EU) 2016/679 (GDPR) entered into force, in July 30, 2019 the Greek Data Protection Authority (DPA) published its first Decision exercising the corrective powers conferred on it under the GDPR. This is Decision 26/2019 (1) which imposes a fine of €150,000 on the company 'PricewaterhouseCoopers Business Solutions S.A.' (PwC BS) for selection and application of inappropriate legal basis for the processing of employee data and for violation of the principle of accountability. In the meantime, the DPA had been investigating compliance of certain large organisations in the insurance, finance and e-commerce business and public sector bodies and had also issued some decisions enforcing GDPR provisions, mainly giving warnings to controllers.*

A useful precedent

▪ *This case set a useful precedent on how a controller and processor can best prepare for an audit by the DPA and also how they can best deal with such an audit. The DPA made it clear that where the controller has doubts concerning the lawfulness of the processing, the controller must refrain from processing until compliance is ensured.*

Documentation

▪ *The DPA highlighted that documentation is a key element of the accountability principle, emphasising that the authority "attaches particular importance to the fact that the controller did not provide any evidence of internal compliance which would indicate the documentation of the choice of an appropriate, according to the controller, legal basis".*

Take corrective measures

▪ *In case of non-compliance, corrective measures must be taken as soon as possible and ideally before the conclusion of the DPA audit. The DPA considered as a sanction evaluation factor the fact that the controller had failed to take corrective measures, despite having expressed to the DPA the intention to do so.*

Ask for expert opinion and assistance

▪ *It becomes apparent that obtaining expert opinion and assistance from the very beginning of the GDPR compliance procedure and also for the needs of a DPA audit can be a factor that will determine likelihood and nature of sanctions.*

(1) An official summary of Decision 26/2019 is available here: https://www.dpa.gr/pls/portal/docs/PAGE/APDPX/ENGLISH_INDEX/DECISIONS/SUMMARY%20OF%20DECISION%2026_2019%20(EN).PDF

GEORGE A. BALLAS & THEODORE KONSTANTAKOPOULOS

greece@lexing.network

▪ En 2019, l'actualité concernant la protection des données en Hongrie s'est cristallisée autour de nouvelles mesures visant à peaufiner certaines normes de protection des données, mais aussi et surtout, du paquet sur la protection des données. Ce paquet, qui amende plusieurs lois sectorielles, vise à assurer a mise en conformité du droit national avec le RGPD. En ce qui concerne la pratique de l'autorité hongroise de protection des données (la « NAIH »), il n'existe pas de lignes directrices spécifiques guidant son examen des cas qui lui sont soumis, mais on peut relever que sa cible principale reste les sociétés multinationales et les responsables du traitement de données qui procèdent au traitement de quantités importantes de données ou de données sensibles. S'agissant des sanctions, les amendes imposées jusqu'à présent vont de 500.000 à 1.000.000 forint hongrois (soit de 1.500 à 3.000 euros), ce qui est nettement inférieur aux montants infligés par les autorités de protection des données des autres États membres de l'UE. La NAIH réalise des contrôles principalement à la suite de plaintes individuelles ou en cas de violation de données à caractère personnel.

▪ Les thématiques suivantes seront particulièrement à surveiller en cas de contrôle de la NAIH :

Consentement à recevoir de la prospection commerciale (2018 septembre) (1)

▪ La NAIH a émis un avis sur la question de savoir si les responsables du traitement sont autorisés à accorder des avantages aux personnes concernées qui donnent leur consentement à recevoir des messages de prospection commerciale. En reprenant essentiellement les lignes directrices du groupe de l'Article 29 (désormais appelé « CEPD ») sur ce sujet, la NAIH a répondu par la positive, à condition cependant que cet avantage n'ait pas pour effet d'entraver le libre choix de la personne concernée de donner son consentement. En outre, l'avantage accordé ne peut pas limiter le droit de la personne concernée de retirer son consentement.

(1) https://www.naih.hu/files/NAIH_2018_3581.pdf

▪ La NAIH évoque également la proposition de règlement « vie privée et communications électroniques » et les changements que ce texte pourrait apporter en la matière. Cela donne à penser que la NAIH suit de près l'évolution de la situation dans ce domaine et compte appliquer ce futur règlement au plus vite.

Copie de documents (2019 octobre) (2)

▪ La NAIH a émis un avis sur la copie des pièces d'identité. L'autorité hongroise a souligné que les sous-traitants ne peuvent faire des copies que sous réserve du respect des principes de limitation des finalités et de minimisation des données. En outre, la copie de pièces d'identité n'est pas nécessaire s'il est possible de réaliser les finalités du traitement sans faire de cette copie et qu'il existe d'autres méthodes moins intrusives pour protéger la vie privée de la personne (par exemple, le contrôle de l'identité par le principe dit des « quatre yeux »). La copie

(2) https://www.naih.hu/files/Adatved_allasfoglalas_2018-3654-2-V-okmanymasolas.pdf

de pièce d'identité n'est légitime que si un tel traitement de données est prescrit par la loi.

Liste des activités de traitement nécessitant une analyse d'impact (2018 décembre) (3)

(3) https://www.naih.hu/files/GDPR_35_4_lista_HU_mod.pdf

▪ La NAIH a publié une liste des activités de traitement pour lesquelles elle estime qu'une analyse d'impact relative à la protection des données (AIPD) est nécessaire. La liste est très longue et inclut des activités évidentes, comme le profilage, mais aussi d'autres activités, telles que les vérifications de crédit, le traitement des données biométriques ou génétiques, le scoring sur la base de données à caractère personnel, l'utilisation de compteurs intelligents, le traitement des données GPS ou encore le traitement des données via les nouvelles technologies.

Droit à l'oubli (2019 mars) (4)

(4) https://www.naih.hu/files/Adatved_allasfoglalas_NAIH_2019_2450_adathordozo_megsemmisites.pdf

▪ La NAIH a émis un avis sur les pratiques d'effacement des données mises en œuvre par les employeurs. Un employeur, à l'instar des autres responsables du traitement, est autorisé à traiter des données à caractère personnel sou réserve de justifier d'une base juridique et d'une finalité de traitement appropriées. L'employeur doit veiller à effacer les données à caractère personnel afin qu'aucune donnée ne puisse être restaurée (par exemple, la simple suppression de données du disque dur ne suffit pas, et l'employeur doit utiliser un programme adéquat). A cet effet, il doit prévoir des délais de conservation spécifiques et mettre en mesures d'effacement des documents.

Adoption du paquet de protection des données par le Parlement (2019 avril) (5)

(5) http://www.kozlonyok.hu/nkonline/MKPDF/hiteles/MK1906 3.pdf

▪ Le Parlement hongrois a adopté une loi modifiant plusieurs textes relatifs à la protection des données dans différents secteurs. Cette loi apporte ainsi des changements dans le domaine du droit du travail, de la vidéosurveillance, de la prospection commerciale, de la réglementation des copropriétés, etc. visant principalement à adapter les dispositions nationales actuelles au regard de l'esprit du RGPD. En effet, le RGPD requiert :

- une plus grande responsabilité en matière de traitement des données,
- un contrôle accru au bénéfice des personnes concernées.

▪ De manière générale, les amendements apportés offrent une plus grande souplesse aux responsables du traitement, au prix toutefois de l'accroissement du nombre d'obligations dont ils doivent s'acquitter, telles que la mise en balance des intérêts et la surveillance constante de la pertinence du traitement des données.

MIKLOS ORBAN

hungary@lexing.network

▪ *The main data protection news in Hungary in the past year cover the data protection package on several sectoral laws to implement GDPR and new measures to fine tune data protection standards. As for the practice of the Hungarian data protection authority there is no specific guideline on the direction of cases examined by the authority. The authority acts mainly upon individual complaints, however we observed that the main target of the authority remains multinational companies and data controllers processing significant amount or sensitive data. As for the fining practice of authority, the fines make for HUF 500,000 - 1,000,000 (EUR 1,500 – 3,000) range, significantly lower than other EU state's data protection authorities. A general trend in fining reflects that the authority investigates and acts upon mainly individual complaints and personal data breaches.*

Consent in direct marketing scenarios (2018 September) (1)

(1) https://www.naih.hu/files/NAIH_2018_3581.pdf

▪ *The Hungarian data protection authority ("HDPA") issued an opinion on whether data controllers are allowed to give some kind of advantage to data subjects if they give consent to receive direct marketing messages. By basically repeating and summarising the opinion of the WP29 on the topic, the HDPA underlined that such advantage can be given but it cannot mount to an extent it would hinder the free choice of the data subject to give consent. The advantage cannot limit the data subject's right of withdrawal.*

▪ *Most importantly, the HDPA draw attention to the e-Privacy Directive and the changes it can bring about regarding the matter. This suggests that the HDPA is paying close attention to the developments in the field and will apply the Directive as soon as it can.*

Document copying (2019 October) (2)

(2) https://www.naih.hu/files/Adatved_allasfoglalas_2018-3654-2-V-okmanymasolas.pdf

▪ *The Hungarian data protection authority issued its opinion on making copies of personal IDs. The authority pointed out that data processors can make copies only in line with the principles of purpose limitation and data minimisation. Data processors must accept IDs because data processors can meet data processing purpose without making copies and there are other less intrusive methods to the privacy of the individual (e.g. check of ID by "four eyes" principle). Copying IDs is legitimate only if such data processing is prescribed by law.*

List of data processing activities requiring impact assessment (2018 December) (3)

(3) https://www.naih.hu/files/GDPR_35_4_lista_HU_mod.pdf

▪ *The Hungarian data protection authority issued its list on the data processing activities for which it deems prior data protection impact assessment to be necessary. The list is considerably extensive including obvious activities like profiling but also listing items such as credit checks, processing biometric or genetic data, scoring on the basis of personal data, using smart meters, processing GPS data or data processing via new technologies.*

Right to be forgotten (2019 March) (4)

▪ *The Hungarian data protection authority issued its opinion on the erasure practices with regard to employers. The employer, as well as other data controllers, can process personal data with the appropriate legal basis and data processing purpose. The employer must erase personal data so that no data can be restored (e.g. simple deleting data from hard drive does not suffice, the employer must use a programme). The employer must arrange for storage times and document erasures.*

(4) https://www.naih.hu/files/Adatved_allasfoglalas_NAIH_2019_2450_adathordozo_megsemmisites.pdf

Data protection package passed by the Parliament (2019 April) (5)

▪ *A law has been approved by the Parliament that enacts several amendments to several acts touching upon data protection issues. The act provides for changes in the sphere of labour law, CCTV surveillance, direct marketing, condominium regulation etc. mainly focusing on accommodating these laws to the nature of the GDPR:*

- *more responsibility for data processing,*
- *more control for data subjects,*

(5) http://www.kozlonyok.hu/nkonline/MKPDF/hiteles/MK19063.pdf

▪ *As a general rule, the amending act provides for more flexibility for data controllers, however, at the cost of more obligations such as balancing tests and constant surveillance of data processing interests.*

MIKLOS ORBAN

hungary@lexing.network

▪ Depuis le mois de mai 2019, l'autorité italienne de protection des données a réalisé de nombreux contrôles, principalement dans le secteur de la grande distribution. Ces contrôles, menés de manière rigoureuse, sont une source d'enseignements importants pour tous les organismes qui, soucieux de respecter la règlementation en matière de protection des données, ont investi des ressources considérables pour assurer leur conformité au RGPD.

▪ Pour bien se préparer à un contrôle de l'autorité, il est nécessaire de prendre en compte certains points de vigilance.

▪ Soignez votre accueil. Les agents de l'autorité vont tout d'abord se présenter à l'accueil de votre entreprise : vos réceptionnistes connaissent-ils le nom de l'autorité de contrôle ? Savent-ils ce qu'est le RGPD, et qui est le DPD au sein de votre entreprise ? N'oubliez pas que vos agents d'accueil et vos standardistes sont les premiers membres de votre entreprise qui entreront en contact avec les agents missionnés par l'autorité. Il est donc essentiel de les (in)former correctement pour marquer des points dès le début des opérations de contrôle.

▪ Par ailleurs, lorsque les agents de l'autorité arrivent ou attendent dans votre hall d'accueil, ils risquent de porter leur attention sur leur environnement immédiat. La plupart des entreprises consignent le nom des visiteurs dans un registre ou disposent de systèmes de vidéosurveillance dans leurs locaux ou à l'entrée de leur immeuble. Si tel est le cas, la règlementation impose à l'entreprise de se doter d'un formulaire ou d'une notice pour fournir aux visiteurs toutes les informations requises par le RGPD. En outre, le CEPD a élaboré des lignes directrices précises concernant la vidéosurveillance. Votre entreprise dispose-t-elle de panneaux affichés de façon visible et de formulaires destinés à informer les personnes concernées de l'existence de ce dispositif et de leurs droits à l'égard des enregistrements vidéo ou des inscriptions portées dans le registre ?

▪ Ce sont là les premiers éléments que remarqueront les agents de l'autorité qui viendront vous contrôler, et il est primordial d'y attacher de l'importance, aussi minimes que ceux-ci puissent paraître de prime abord. Comme souvent, le diable est dans les détails !

Liste de 19 points. Lors des contrôles qu'elle a effectués jusqu'à présent, l'autorité italienne a présenté aux organismes contrôlés une liste constituée de dix-neuf points (1). Quelques-uns des thèmes abordés s'attachent à vérifier le respect d'un certain formalisme, tandis que d'autres concernent des thèmes plus substantiels.

▪ Au niveau de la forme, il est demandé copie de certains documents tels que :

- le registre des activités de traitement (art. 30 du RGPD), les contrats de sous-traitance conclus avec les éventuels sous-traitants, l'acte de désignation du délégué à la protection des données, etc.

▪ Au niveau du fond, il est notamment demandé de justifier des mesures mises en œuvre pour assurer la conformité au RGDP :

- Avez-vous, à l'instar de nombreuses entreprises, instauré une équipe ou un service spécialement dédié à la gestion des actions requises par le RGPD ? Si oui, avez-vous documenté les activités de cette équipe ? Par exemple, avez-vous constitué une liste des membres de votre personnel

(1) Vous pouvez consulter la liste des 19 points ici en italien et ici en anglais

qui la composent ? Des comptes rendus de réunions sont-ils dressés ? Les ressources qui lui sont allouées sont-elles répertoriées… ?

▪ L'autorité cherche également à comprendre comment la protection des données à caractère personnel s'articule dans votre organisation interne :

- Votre entreprise a-t-elle attribué des fonctions et des responsabilités précises en matière de protection des données à certains collaborateurs ? Avez-vous une liste des salariés qui ont accès aux données à caractère personnel ? Tenez-vous cette liste à jour ? Ces salariés ont-ils reçu une formation spécifique sur le RGPD ? Connaissent-ils les caractéristiques de leur niveau d'habilitation en termes d'accès et d'usage de données à caractère personnel ? Comment l'entreprise vérifie-t-elle le respect de ces habilitations ?
- Avez-vous effectué une analyse d'impact relative à la protection des données ? Sur quelles opérations de traitement cette AIPD portait-elle précisément ? Quelles procédures ont été mises en place pour garantir le respect des droits des personnes concernées, et notamment leur droit d'accès ?

▪ Enfin, plusieurs points portent naturellement sur les mesures de sécurité, thématique on ne peut plus importante et sensible.

▪ Hormis quelques questions spécifiquement ciblées pour les grandes entreprises commerciales, la majorité d'entre elles s'adressent à toutes les organisations, quelle que soit leur taille. Cette liste de 19 points peut dès lors être utilement exploitée par l'ensemble des responsables du traitement afin de se préparer à un contrôle de conformité au RGPD par l'autorité italienne.

Conclusion En substance, ce qu'il faut retenir c'est que l'autorité veut avant tout prendre connaissance des différentes actions que vous avez mis en place pour vous conformer au RGPD et vérifier votre respect du principe de responsabilité, en consultant la documentation que vous avez compilé à cette fin tout au long de votre démarche de conformité.

▪ La liste des 19 points décrite plus haut a été élaborée en fonction des contrôles réalisés depuis moins d'un an après l'application du RGPD, et est susceptible d'évoluer au fur et à mesure des activités d'enquête de l'autorité. Si pour l'instant elle reste assez générale en mettant l'accent sur la mise en place des différents systèmes et procédures internes au regard du RGPD, il est probable que les contrôles futurs auront une granularité plus fine et un caractère plus pragmatique. Il faudra donc s'attendre par la suite à se voir poser des questions précises, telles que : votre registre des activités de traitement est-il mis régulièrement à jour ? Combien de demandes d'accès avez-vous reçues et comment les avez-vous traitées ? Avez-vous reçu des demandes concernant le droit à la portabilité des données ?...

▪ Gardez-bien à l'esprit que le respect du RGPD ne peut être garanti par des actions ponctuelles, mais par un processus permanent, continu. Il est capital de contrôler les activités de votre l'entreprise tout au long du cycle de vie de toutes vos données pour s'assurer qu'aucune erreur ne soit commise. A défaut, vous risquez d'apprendre, à vos dépens, combien ces erreurs peuvent être lourdes de conséquence avec le RGPD.

RAFFAELE ZALLONE

italy@lexing.network

▪ *Starting last May the Italian DPA has conducted several audits and inspections, mostly in large retailers; these inspections have been conducted in depth, and from these experiences there are significant lessons to be learned, mainly for those customers that have invested a significant amount of resources to be compliant to the GDPR.*

▪ *The following is a short list of the main areas to check, in order to have everything taken care of in case of possible inspections.*

▪ *First things first. The DPA arrives at the reception of your company: do your receptionist know who the DPA is, what the GDPR is and who the DPO is? The receptionists are the first employees the authority shall meet, and their education on this point is key to start the audit in a positive way. Most companies record the names of the visitors that enter their premises: in this case an information form has to be prepared, so that third party visitors shall receive all information required under the GDPR.*

▪ *Most companies have video-surveillance systems in their premises and/or at the entrance. The EDPB has issues clear guidelines on what to do in this case, so the point is: are all the signs and information forms available and visible?*

▪ *These are just the initial steps to take, since these are the first things that the officials coming to inspect you shall notice, and it is very important that the companies appear to be compliant also in small things.*

▪ *List of 19 points. In the inspections it has carried out so far the Italian DPA has presented a list of requests in nineteen points (1). Some of them are merely formal, other are more relevant.*

(1) Read the 19-point list here in Italian and here in English

- *The formal requests are related to the documentation: it is requested to show the record of processing activities (sec. 30 of the GDPR), if the controller has appointed processors and the related contracts, if there is a DPO, etc.*

▪ *The most significant ones are related to the evidence of the work done:*

- *Is there documentation showing the meetings and the efforts made? Many companies have created a project office to manage all the activities requested by the GDPR: have you documented these activities? Do you have the list of managers and employees that have been involved?*

▪ *The inspectors also insisted in trying to understand the internal privacy organization:*

- *Has the company assigned specific privacy-related roles and responsibilities to managers or employees? Who are the employees that have access to*

personal data and does the company has a list of such employees? Have they ever had any education on the GDPR other than formal instructions? Do they know what data they can access and use in their assignment, and how does the company control that they access only such data?

- *Has any DPIA been performed and on what processing operations? What procedures have been implemented to guarantee full respect of the rights of the data subject in case of access requests or other similar requests?*

▪ *Finally, the list includes several questions on the security measures, which again is a very important and sensitive subject.*

▪ *Many questions relate specifically to large retail companies; many other are of interest for everyone and the basic point for a review of what is available for every controller, so that a potential inspection can find you ready and well prepared.*

▪ *Conclusion. The net of all this is the following: the DPA wants to see what has been done to comply with the GDPR and see if the accountability principle has been respected. Also, they want to see documentation that supports the implementation of the compliance project, so that they can be satisfied that the law is applied.*

▪ *These inspections have been carried out one year after the coming into force of the GDPR; it is likely that future inspections shall focus on the day-to-day operations with respect to the GDPR, i.e.: the record of processing activities has it been updated? How many access requests have you received and how you dealt with them? Have you received any requests for portability?*

▪ *In other words, compliance with the GDPR is not a one-shot deal, but a continuing process, and it is key to continue to control the company's operations to make sure no mistake is made, since mistakes in this field can be very dangerous.*

RAFFAELE ZALLONE

italy@lexing.network

LEXING NETWORK

PAYS / COUNTRY	CABINET / FIRM	CONTACT	TELEPHONE	EMAIL
Afrique du Sud *South Africa*	Michalsons	John Giles	+27 (0) 21 300 1070	south-africa@lexing.network
Allemagne *Germany*	Beiten Burkhardt	Andreas Lober	+49 69 756095-0	germany@lexing.network
Australie *Australia*	Gadens	Dudley Kneller	+61 438 363 443	australia@lexing.network
Belgique *Belgium*	Lexing Belgium	Jean-François Henrotte	+32 4 229 20 10	belgium@lexing.network
Canada *Canada*	Langlois avocats, S.E.N.C.R.L.	Jean-François De Rico	+1 (418) 650 7000	canada@lexing.network
Chine *China*	Jade & Fountain PRC Lawyers	Jun Yang	+86 21 6235 1488	china@lexing.network
Costa Rica *Costa Rica*	Lexing Costa Rica	Gabriel Lizama	+506 2253-1726	costa-rica@lexing.network
Côte d'Ivoire *Ivory Coast*	Imboua Kouao Tella & Associés	Annick Imboua-Niava	+ 225 22 44 74 00	ic@lexing.network
Espagne *Spain*	Lexing Spain	Marc Gallardo	+ 34 93 476 40 48	spain@lexing.network
États-Unis *USA*	DataMinding Legal Services	Françoise Gilbert	+1 650-804-1235	usa@lexing.network
France *France*	Alain Bensoussan-Avocats Lexing	Alain Bensoussan	+33 1 82 73 05 05	france@lexing.network
Grèce *Greece*	Ballas, Pelecanos & Associates L.P.C.	George A. Ballas	+ 30 210 36 25 943	greece@lexing.network
Hongrie *Hungary*	OPL - Orbán & Perlaki	Miklos Orban	+36 1 244 8377	hungary@lexing.network
Inde *India*	Poovayya and Co	Siddhartha George	+91 80 4115 6777	india@lexing.network
Israël *Israel*	Appelfeld & Co	Ilanit Appelfeld	+ 972 3 60 98 099	israel@lexing.network
Italie *Italy*	Studio Legale Zallone	Raffaele Zallone	+ 39 (0) 229 01 35 83	italy@lexing.network
Japon *Japan*	Hayabusa Asuka Law Office	Koki Tada	+81 3 3595 7070	japan@lexing.network
Liban *Lebanon*	Kouatly & Associates	Rayan Kouatly	+ 961 175 17 77	lebanon@lexing.network
Maroc *Morocco*	Fayçal Elkhatib et Associés S.C.P.A	Hatim Elkhatib	+212 5 39 94 05 25	morocco@lexing.network
Mexique *Mexico*	Carpio, Ochoa & Martínez Abogados	Enrique Ochoa De González Argüelles	+ 52 55 25 91 1070	mexico@lexing.network
Norvège *Norway*	Advokatfirmaet Føyen Torkildsen AS	Arve Føyen	+47 21 93 10 00	norway@lexing.network
Nouvelle-Calédonie *New Caledonia*	Cabinet Franck Royanez	Franck Royanez	+ 687 24 24 48	nc@lexing.network
Pologne *Poland*	Traple Konarski Podrecki i Wspòlnicy	Xawery Konarski	(+48) 12 426 05 30	poland@lexing.network
Portugal *Portugal*	Alves Pereira & Teixeira de Sousa	João P. Alves Pereira	+ 351 21 370 01 90	portugal@lexing.network
République tchèque *Czech Republic*	Rowan Legal	Josef Donát Michal Nulíček	+420 224 216 212	czechrepublic@lexing.network
Royaume-Uni *United Kingdom*	Preiskel & Co LLP	Danny Preiskel	+ 44 (0) 20 7332 5640	uk@lexing.network
Russie *Russia*	ALRUD	Maria Ostashenko	+ +7 495 234 96 92	russia@lexing.network
Sénégal *Senegal*	SCP Faye & Diallo	Mamadou Seye	:(+221) 33 823 60 60	senegal@lexing.network
Slovaquie *Slovakia*	Rowan Legal	Josef Donát Michal Nulíček	+420 224 216 212	slovakia@lexing.network
Suisse *Switzerland*	Sébastien Fanti	Sébastien Fanti	+ 41 (0) 27 322 15 15	switzerland@lexing.network

La JTIT est éditée par Alain Bensoussan Selas, société d'exercice libéral par actions simplifiée, 58 boulevard Gouvion-Saint-Cyr, 75017 Paris, président : Alain Bensoussan. Directeur de la publication : Alain Bensoussan – Responsable de la rédaction : Isabelle Pottier
Diffusée uniquement par voie électronique – gratuit– ISSN 1634-0701
Abonnement à partir du site : https://www.alain-bensoussan.com/outils/abonnement-petit-dejeuner-debat/