Ethikosletter

01

EDITORIAL

Making business ethical

The legislative inflation we have been facing since 2007 is sometimes dizzying.

The multiplication of sources of law, both external and internal, the emergence of new fields, the appearance of new constraints and the globalized environment in which we must navigate today are all factors that explain both the increase in the number of laws passed and the lengthening of legislative and regulatory texts.

The health crisis we are currently experiencing should logically accelerate this dynamic.

Aware of the growing difficulties to which your company is subject, we thought it would be useful to lend you a hand by issuing our quarterly newsletter.

Born out of a concern for simplification in an increasingly complex legislative environment, our newsletter contains an overview of recent legislative developments in business law, as well as a compilation of recent briefing notes and articles published on our LinkedIn page.

In this way, we also hope to make you a little more aware of the benefits of ethics in business by showing you that economic growth and respect for values are not incompatible.

Miguel **Mairlot**
Partner @Ethikos

SUMMARY

1/ LEGAL WATCH

This section contains a very selective overview of the main regulatory developments adopted in business law during the past quarter.

Ethikos is at your disposal to assist you with the 'to do's' mentioned below.

As this is our first newsletter, we took the liberty of listing below new legislation that was adopted before the last quarter.

a. The B2B Act

Relevant for: all businesses

Summary:

The Belgian Act of 4 April 2019 (or 'B2B Act') inserts three new sets of rules (see below) for B2B relationships in the Code of Economic Law. These rules already existed to some extent for the B2C relationships.

(i) Prohibition of abuse of economic dependence

The B2B Act prohibits an enterprise to abuse a position of economic dependence of another enterprise, by which competition on the Belgian market or a substantial part of it can be affected (e.g. by applying towards economic partners dissimilar conditions to equivalent services).

The entry into force of this part of the Act has been postponed until 1 December 2020 at the latest.

(ii) Prohibition of unfair contract terms

The B2B Act prohibits terms that create a significant imbalance between the rights and obligations of the parties.

In addition to this general prohibition, the B2B Act contains:

a. A **'blacklist'** of terms, which are prohibited without further assessment.

   E.g. the term gives to one party the unilateral right to interpret any term in the contract.

b. A **'grey list'** of terms presumed to be unfair and prohibited unless there is proof to the contrary.

   E.g. the term gives to one party the unilateral right to interpret any term in the contract.

Until a Royal Decree states otherwise, these new rules do not apply to financial services or public procurement contracts.

This part of the Act will be applicable as from 1 December 2020, but only for contracts concluded, renewed, or modified after this date.

(iii) Prohibition of unfair market practices

Finally, the B2B Act introduces a distinction between misleading and aggressive market practices for unfair market practices between businesses.

The B2B Act has already been heavily criticized, among others because it will - almost inevitably - give rise to interpretation issues and because it considerably limits the contractual freedom of enterprises.

Main to do's:

Given the heavy penalties provided for by the B2B Act (prohibited term declared null and void and/or high fines), it is paramount to:

- Review all the existing B2B contracts to detect and remove any abuse of economic dependence.
- Review all the B2B contractual templates (including terms and conditions) to remove any prohibited terms.
- Align the procurement processes (including the review of the contract of the service providers) with the new rules.

b. EBA Guidelines on outsourcing arrangements

Relevant for: credit and payment institutions

Summary:

In February 2019, the EBA (European Banking Authority) published its 'Guidelines on outsourcing arrangements'. The NBB (National Bank of Belgium) has implemented the guidelines through a circular of July 2019. This circular repeals and replaces the previous texts in this respect, including the Circular PPB 2004/05.

The new rules entered into force on 30 September 2019.

Main to do's:

These Guidelines and circular require extensive compliance work, including:

- The drafting of an outsourcing policy.
- The alignment of the procurement processes with the new rules.
- The assessment of all the contracts with service providers, among others to determine whether they can be qualified as (critical) outsourcing.
- The review of all the outsourcing contracts.
- The completion of an outsourcing register.

Be sure to be compliant at the latest for 31 December 2021, because the NBB announced in its circular that it could request the outsourcing register in the first semester of 2022.

c. Implementation of the Shareholder Rights Directive II

Relevant for: listed companies, intermediaries (credit institutions, investment firms, and central securities depositaries), institutional investors and asset managers, proxy advisors

Summary:

The Belgian Act of 28 April 2020 transposes into Belgian law the 'Shareholder Rights Directive II'. Most of the provisions of the Act entered into force on 16 May 2020.

The new rules introduced by this Act aim to strengthen the position and encourage the long-term engagement of shareholders of listed companies.

The main changes concern:

(i) Identification of shareholders

The Act allows listed companies to identify their shareholders, to enable direct communication with them. To this end, a certain number of obligations to communicate information regarding the identity of shareholders are imposed on intermediaries (credit institutions, investment firms, and central securities depositaries) through which the shares are held.

(ii) Commitment of shareholders

The Act imposes greater transparency on intermediaries by requiring institutional investors and asset managers to publish their shareholder engagement policy and a report on how that policy has been implemented.

(iii) Remuneration policy: the 'say on pay' principle

Shareholders of listed companies have now greater control over executive compensation.

(iv) Proxy advisors

That Act also introduces new obligations to proxy advisors ('conseillers en vote'/'volmachtadviseurs'), among others a public disclosure of the code of conduct which they apply (if any) and disclosure of a report on the application of that code.

(v) Related party transactions

Finally, the new procedure for related party transactions corresponds more or less to the existing procedure for intra-group conflicts of interest (see articles 7: 97 and 7: 116 of the Code of Companies and Associations). Its scope of application is, however, substantially extended.

Please note that this Act is - until now at least - only applicable to companies listed on a regulated market (e.g. Euronext Brussels), and not on the other types of markets (e.g. Euronext Growth, which is an MTF or multilateral trading facility).

Main to do's:

• For the listed companies:

- Review the remuneration policy and remuneration report to align them with the new rules.
- Align the procedures concerning third party transactions with the new rules.

• For the intermediaries (credit institutions, investment firms, and central securities depositaries):

- When the listed company requires it, communicate information about the identity of the shareholders.

• For the institutional investors and asset managers:

- Comply with the new obligations concerning the engagement policy and investment strategy.

• For the proxy advisors

- Comply with the new disclosure obligations.

2/ ARTICLES

This section contains the articles published by Ethikos during the past quarter.

a. COVID-19: the processing of personal data in the employment context
b. COVID-19 and AML (in French)
c. DPO requirements checklist

a. COVID-19: the processing of personal data in the employment context

The rapid spread of the COVID-19 confronts European countries with radical choices. In some Member States, governments envisage using mobile location data as a possible way to monitor, contain, or mitigate the spread of COVID-19. This would imply, for instance, the possibility to geolocate individuals or to send public health messages to individuals in a specific area by phone or text message.

In a recent statement, the European Data Protection Board declared that 'the fight against communicable diseases is a valuable goal shared by all nations and therefore, should be supported in the best possible way. It is in the interest of humanity to curb the spread of diseases and to use modern techniques in the fight against scourges affecting great parts of the world'.

In the employment context, the processing of personal data may also be necessary for compliance with a legal obligation to which the employer is subject such as obligations relating to health and safety at the workplace, or to the public interest, such as the control of diseases and other threats to health.

Data protection rules (such as the GDPR) do not hinder measures taken in the fight against the COVID19 pandemic. The GDPR foresees derogations to the prohibition of processing of certain special categories of personal data, such as health data, where it is necessary for reasons of substantial public interest in the area of public health, based on Union or national law, or where there is the need to protect the vital interests of the data subject.

Even in these exceptional times, organizations subject to the GDPR should not lose sight of their obligations to act in compliance with the fundamental rights to privacy and personal data protection.

Supervisory authorities across Europe have the power to impose administrative fines for infringements of the regulation up to € 20,000,000 or in the case of an undertaking, 4 % of the total worldwide annual turnover - whichever is higher, and it is reasonable to assume that particular attention will be paid by these authorities to the collection and processing of sensitive data, such as health data.

Therefore, several considerations should be considered by organizations subject to the GDPR to guarantee the lawful processing of personal data of their employees in the context of the fight against the COVID-19.

- Can an employer require visitors or employees to provide specific health information in the context of COVID-19?

The application of the principle of proportionality and data minimization is particularly relevant here. The employer should only require health information to the extent that national law allows it.

- Is an employer allowed to perform medical check-ups on employees?

The answer relies on national laws relating to employment or health and safety. Employers should only access and process health data if their legal obligations require it.

- Can an employer disclose that an employee is infected with COVID-19 to his colleagues or externals?

Employers should inform staff about COVID-19 cases and take protective measures but should not communicate more information than necessary. In cases where it is necessary to reveal the name of the employee(s) who contracted the virus (e.g. in a preventive context) and the national law allows it, the concerned employees shall be informed in advance and their dignity and integrity shall be protected.

- What information processed in the context of COVID-19 can be obtained by the employers?

Employers may obtain personal information to fulfill their duties and to organize the work in line with national legislation.

b. COVID-19 et lutte anti-blanchiment: mises en garde et attentes des régulateurs

La crise sanitaire causée par l'épidémie du Covid-19 a conduit les établissements financiers soumis à la loi relative à la prévention du blanchiment de capitaux et du financement du terrorisme et à la limitation de l'utilisation des espèces (ci-après «loi anti-blanchiment») à adopter des mesures visant à assurer la continuité de leurs services.

Consciente du fait que ces mesures, notamment le télétravail systématique et généralisé pendant une longue période, ont et auront encore des conséquences importantes sur l'accomplissement de nombreuses tâches relatives à la prévention du blanchiment de capitaux et du financement du terrorisme (LBC/FT), la Banque Nationale de Belgique (ci-après la «BNB») a émis, le 7 avril 2020, une communication afin d'encourager les établissements financiers à concentrer les ressources qu'ils allouent à cette prévention sur les tâches qui sont les plus nécessaires pour maintenir un niveau élevé d'efficacité de ces mécanismes.

Dans sa communication, la BNB attire également l'attention des établissements financiers sur les communications officielles publiées à cet égard par l'Autorité Bancaire Européenne, par le GAFI et par la CTIF.

La présente note a pour objectif de fournir, sous forme de questions, des éclaircissements sur les attentes et les différentes mises en garde émises par les autorités susmentionnées.

- Les établissements financiers bénéficient-ils d'un report pour la communication du rapport d'activité de l'AMLCO et du questionnaire périodique 2020?

Compte tenu des circonstances exceptionnelles, la BNB a décidé de reporter du 30 juin 2020 au 31 août 2020, soit de deux mois, la date limite pour lui communiquer, via eCorporate, copie du rapport d'activité de l'AMLCO et pour répondre, via OneGate, au questionnaire périodique 2020 relatif à la prévention du blanchiment de capitaux et du financement du terrorisme.

- Quel est l'impact du télétravail sur l'accomplissement des tâches relatives à la prévention du blanchiment de capitaux et du financement du terrorisme (LBC/FT)?

La B.N.B. est consciente des difficultés auxquelles sont actuellement confrontés les établissements financiers lors de l'accomplissement de leurs tâches liées à la LBC/FT. Tenant compte de ces difficultés, la B.N.B. encourage ces établissements financiers à concentrer les ressources dont elles disposent pour la mise en œuvre de leurs mécanismes internes de LBC/FT sur les tâches qui sont les plus nécessaires pour maintenir un niveau élevé de détection et d'analyse des opérations atypiques, ainsi que de déclaration des opérations, fonds et faits suspects à la CTIF, conformément aux obligations légales.

- Cela veut-il dire que les établissements financiers sont dispensés de se conformer au reste de leurs obligations légales en matière de LBC/FT durant la crise sanitaire?

Nous ne le pensons pas. La B.N.B. invite uniquement les établissements financiers qui relèvent de ses compétences de contrôle à prendre les mesures nécessaires pour maintenir pleinement effectifs et efficaces tant leurs mécanismes de contrôle des opérations de leurs clients que leurs cellules de prévention du BC/FT, pour leur permettre de détecter rapidement les opérations atypiques susceptibles d'être liées à de telles activités criminelles, de les analyser avec efficacité, et de déclarer sans retard à la CTIF les opérations, fonds et faits que cette analyse les conduirait à considérer suspects d'être liés au blanchiment de capitaux. Si les établissements financiers doivent allouer leurs ressources en priorité à l'accomplissement de ces tâches, cela ne veut toutefois pas dire que ceux-ci sont dispensés de se conformer aux restes de leurs obligations légales issues de la loi anti-blanchiment. On comprendrait mal d'ailleurs que les autres mesures préventives telles que l'évaluation globale des risques, l'identification ou de la vérification de l'identité des clients (KYC), l'obligation de vigilance ou les différentes obligations de reporting auxquelles sont soumises les établissements financiers, ne continuent pas à s'appliquer dans la mesure où celles-ci sont nécessaires au bon accomplissement des mesures de détection et d'analyse des opérations atypiques, ainsi que de déclaration des opérations, fonds et faits suspects à la CTIF.

- Doit-on s'attendre à un changement de comportement de la part des autorités de contrôle durant la crise sanitaire?

L'approche fondée sur les risques établie par la loi anti-blanchiment offre autorités compétentes chargées de la surveillance des établissements financiers une certaine flexibilité pour planifier leurs activités de surveillance. Cela peut entraîner, par exemple, un report temporaire des inspections sur place, même après la levée des restrictions en matière de circulation, la tenue de réunions et inspections virtuelles le cas échéant, ou un report des délais prévus pour la soumission des questionnaires périodiques. A ce jour, la B.N.B. a uniquement fait usage de cette possibilité de report pour la communication du rapport d'activité de l'AMLCO et du questionnaire périodique 2020. Il n'est toutefois pas exclu que la B.N.B. adopte d'autres mesures temporaires en fonction de l'évolution de la situation.

- À quels types d'activités criminelles les établissements financiers doivent-ils être attentifs durant la crise sanitaire?

La B.N.B. rappelle que, dans les situations de crise, des personnes mal intentionnées et des organisations criminelles s'efforcent systématiquement d'en tirer profit pour déployer leurs activités criminelles afin de s'enrichir de manière illicite en exploitant les peurs toutes légitimes de la population.

À cet égard, l'Autorité Bancaire Européenne constate une recrudescence des cas de cybercriminalité, de fraudes et escroqueries visant les personnes et les entreprises vulnérables, de fausses campagnes de collecte de fonds et de vente de marchandises rationnées à un prix plus élevé.

Le GAFI met en garde contre la publicité et le trafic de médicaments contrefaits, les opportunités d'investissement frauduleuses et les tentatives de phishing qui exploitent les craintes liées aux virus. Selon le GAFI, les «cybercrimes» malveillants ou frauduleux, les collectes de fonds pour de faux organismes de bienfaisance et diverses escroqueries médicales ciblant des victimes innocentes sont susceptibles d'augmenter, les criminels tentant de profiter de la pandémie en exploitant les personnes ayant besoin de soins urgents et en diffusant des informations erronées sur le COVID-19.

La CTIF a, dans un premier temps, attiré l'attention des institutions financières sur les effets à court terme de la crise sanitaire, lesquels se manifestaient essentiellement en matière d'escroqueries liées au commerce de matériel de protection.

- Quels types de criminalités sous-jacentes pourraient être les plus affectées par la crise économique ou avoir le plus de conséquences en matière de blanchiment de capitaux?

Les extorsions de sociétés et d'institutions suite à la paralysie de leur système informatique sont susceptibles d'augmenter fortement. À court terme et parfois peu préparées, les organisations ont dû introduire massivement le télétravail. L'accès au réseau d'une société par ses employés, fréquemment au moyen de leur propre matériel informatique, est vulnérable aux attaques de cybercriminels. Via cet accès, ils peuvent parvenir à paralyser le système informatique de toute une organisation et réclamer ensuite une rançon afin de débloquer le système. Via le phishing, les cybercriminels tentent d'accéder aux codes des clients de la banque, généralement suite à l'envoi d'un mail les dirigeant vers un faux site de la banque. Suite à la fermeture des agences bancaires, des clients plus vulnérables n'ont accès qu'à la plateforme en ligne avec laquelle ils sont moins familiers.

Les cybercriminels pourraient également utiliser la crise du Covid-19 comme prétexte dans leurs mails de phishing dans lesquels ils demandent, au nom de l'institution financière, une mise à jour des données de sécurité sous prétexte de la situation exceptionnelle.

Une augmentation du commerce de drogues en ligne et de la livraison de marchandises par des services de coursiers est prévisible compte tenu de la fermeture des magasins physiques. Concernant l'importation de stupéfiants, la police et la douane ont observé, au cours de la période qui a précédé la limitation des vols internationaux, une forte augmentation des mules dans les aéroports, transportant tant de l'héroïne que de la cocaïne, lesquelles ont été saisies. Au port d'Anvers également, de grandes quantités de cocaïne ont récemment été interceptées.

Les organisations criminelles actives dans l'import de drogues ont vraisemblablement tablé sur une diminution des contrôles à cause des mesures prises suite au Covid-19, et pourraient poursuivre ainsi dans le futur.

Du fait de la fermeture générale des commerces, le cash ne sait plus être injecté au travers de sociétés actives dans des secteurs cash intensive servant de couverture. De même, les versements en espèces auprès d'agences bancaires sont devenus impossible ou attirent directement l'attention. Dans la mesure où le trafic de stupéfiants tourne majoritairement autour du cash, nul doute que des montants importants restent momentanément en-dehors du système financier.

Le relâchement des mesures de restriction et la crise économique constitueront une excellente occasion pour les organisations criminelles de pouvoir blanchir ces fonds. Plusieurs sociétés actives dans l'Horeca ou le commerce auront beaucoup de mal à garder la tête hors de l'eau et seront vulnérables à des reprises par le milieu criminel. En outre, pour ces sociétés, un important chiffre d'affaires en cash sera appréhendé de manière peu critique et pourra être justifié par un 'mouvement de rattrapage' des clients.

L'insécurité économique risque d'engendrer une diminution des prix de l'immobilier. Le blanchiment de fonds issus du trafic de stupéfiants au moyen d'investissements immobiliers se déroulera dès lors de manière plus efficace. Cet effet jouera tant au niveau national qu'international.

Le fait que le matériel de protection Covid-19 se trouve presqu'exclusivement en Chine, forme, compte tenu de l'urgence de la situation, un terreau fertile à diverses formes de corruption.

Certains secteurs, comme la construction, le nettoyage industriel et le transport de marchandises, sont particulièrement exposés à la fraude sociale et fiscale.

La fraude au chômage temporaire consiste pour une société à déclarer les travailleurs en chômage alors qu'ils travaillent.

Le recours à des réservoirs de main d'œuvre non déclarée par des sociétés faisant partie d'un réseau criminel de plusieurs sociétés présentant un profil similaire, qui servent mutuellement de couverture pour rémunérer des travailleurs non-déclarés, sans respecter tout ou partie de leurs obligations sociales et fiscales.

- À quels indicateurs spécifiques les établissements financiers doivent-ils être attentifs durant la crise sanitaire?

L'investissement dans des produits financiers qui deviennent moins attrayants en raison de rendements décroissants, ou des techniques de blanchiment d'argent qui donnent lieu à une augmentation du risque de détection, comme le remboursement anticipé des prêts;

L'accroissement ou le maintien de flux financiers importants dans le chef d'un client actif dans un secteur touché par le ralentissement économique et les mesures d'atténuation COVID-19 (ex. les entreprises du secteur du commerce de détail qui utilisent beaucoup de cash);

Le contournement des mesures d'identification et vérification de l'identité (KYC) par des clients qui exploitent les failles en matière de contrôle interne causées par les situations de travail à distance;

L'utilisation accrue de services financiers en ligne et l'investissement dans des actifs virtuels pour déplacer et dissimuler des fonds illicites;

L'exploitation des mesures de relance économique et des régimes d'insolvabilité comme moyen de dissimuler et blanchir les produits illicites issus d'infraction;

Les personnes qui placent de l'argent en dehors du système bancaire en raison de l'instabilité financière. Cela peut conduire à une utilisation accrue du secteur financier non réglementé, créant des possibilités supplémentaires pour les criminels de blanchir des fonds illicites;

L'utilisation abusive et le détournement de l'aide financière nationale et internationale et du financement d'urgence afin d'éviter les procédures de passation de marchés standard, avec pour conséquence un risque de corruption accru;

La réorientation des criminels et terroristes vers de nouvelles activités à forte intensité de liquidités et vers certains pays en développement, notamment en prétendant frauduleusement être des organisations caritatives pour collecter des fonds en ligne.

- Les établissements financiers sont-ils tenus de plus communiquer avec les autorités de contrôle durant la crise sanitaire?

Dans leurs communiqués officiels, le GAFI et l'Autorité Bancaire Européenne soulignent l'importance des interactions proactives entre les autorités publiques et les entreprises soumises aux obligations de prévention afin d'apporter une réponse adéquate au risque de recrudescence des activités criminelles que la crise sanitaire peut générer.

De ce point de vue, le travail d'analyse des opérations atypiques peut amener les AMLCO à déceler des indices de l'émergence de nouveaux schémas d'activités criminelles sous-jacentes au blanchiment de capitaux qui devraient être portés à la connaissance, non seulement des autorités, mais également de la communauté financière dans son ensemble, afin de les contrer le plus efficacement possible.

Dans de tels cas, indépendamment de la déclaration des opérations, fonds et faits suspects à la CTIF qui demeure bien entendu légalement requise, la B.N.B. invite instamment les AMLCO qui constateraient des indices de ce type à communiquer cette information par la voie de courriers électroniques, tant à la CTIF, à l'adresse info@ctif-cfi.be, qu'à la Banque, à l'adresse supervision.ta.aml@nbb.be.

Dès lors que de telles communications leurs seraient adressées et feraient apparaître la nécessité de partager cette information avec l'ensemble des établissements financiers, la B.N.B. se concertera avec la CTIF afin de procéder à ce partage d'information par la voie qui leur apparaîtra la plus efficace et la plus opportune afin de renforcer les mécanismes de prévention.

c. DPO requirements checklist

On 28 April 2020, the Belgian Data Protection Authority fined a company 50.000 EUR because its DPO was not in a position that is sufficiently free from conflict of interest. The concerned DPO also fulfilled the function of director of audit, risk, and compliance. The full decision of the APD is available here.

You are a DPO and you are concerned about the consequences of this decision? Look at our checklist to ensure that you meet the GDPR requirements.

Requirement[1]	Source	Description
Independence[2]	Recital 97 of GDPR	'Such data protection officers, whether or not they are an employee of the controller, **should be in a position to perform their duties and tasks in an independent manner.'**
	Art. 38(3) of GDPR	'The controller and processor shall ensure that the data protection officer **does not receive any instructions regarding the exercise of those tasks.** He or she shall not be dismissed or penalised by the controller or the processor for performing his tasks. The data protection officer shall directly report to the highest management level of the controller or the processor.'
Involvement	Art. 38(1)	'The controller and the processor shall ensure that the data protection officer **is involved, properly and in a timely manner, in all issues which relate to the protection of personal data.'**
	WP29 DPO Guidelines[3]	'It is crucial that the DPO, or his/her team, is involved **from the earliest stage possible** in all issues relating to data protection.'
		'Ensuring that the DPO is **informed and consulted [...]'**
		'In addition, it is important that the DPO be seen as a discussion partner within the organisation and that he or she be **part of the relevant working groups** dealing with data processing activities within the organisation.'
Necessary resources	Art. 38(2)	'The controller and processor shall support the data protection officer in performing the tasks referred to in Article 39 by **providing resources necessary to carry out those tasks and access to personal data and processing operations, and to maintain his or her expert knowledge.'**

(1) The requirements are listed alphabetically.
(2) See also below 'no conflict of interests'.
(3) Article 29 Data Protection Working Party, *Guidelines on Data Protection Officers*, https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048

	WP29	'Depending on the nature of the processing operations and the activities and size of the organisation, the following resources should be provided to the DPO • **active support** of the DPO's function by senior management • **sufficient time** for DPOs to fulfill their tasks • adequate support in terms of **financial resources, infrastructure (premises, facilities, equipment) and staff** where appropriate • official communication of the designation of the DPO to all staff • **continuous training** • 'Given the size and structure of the organisation, it may be necessary to set up a **DPO team** (a DPO and his/her staff).'
No conflict of interests	Art. 38(6)	'The data protection officer may fulfill other tasks and duties. **The controller or processor shall ensure that any such tasks and duties do not result in a conflict of interests.'**
	WP29	'This entails in particular that the DPO **cannot hold a position within the organisation that leads him or her to determine the purposes and the means of the processing of personal data**. Due to the specific organisational structure in each organisation, this has to be considered case by case. As a rule of thumb, **conflicting positions within the organisation may include senior management positions (such as chief executive, chief operating, chief financial, chief medical officer, head of marketing department, head of Human Resources or head of IT departments)** but also other roles lower down in the organisational structure if such positions or roles lead to the determination of purposes and means of processing. In addition, a conflict of interests may also arise for example if an external DPO is asked to represent the controller or processor before the Courts in cases involving data protection issues. Depending on the activities, size, and structure of the organisation, it can be **good practice** for controllers or processors: • to **identify the positions which would be incompatible** with the function of DPO • to **draw up internal rules** to this effect to avoid conflicts of interests • to **include a more general explanation** about conflicts of interests • to **declare that their DPO has no conflict of interests** concerning its function as a DPO, as a way of raising awareness of this requirement • to **include safeguards in the internal rules of the organisation** and to ensure that the vacancy notice for the position of DPO or the service contract is sufficiently precise and detailed to avoid a conflict of interests. In this context, it should also be borne in mind that conflicts of interests may take various forms depending on whether the DPO is recruited internally or externally.'

Obligation of secrecy	Art. 38(5)	'The data protection officer **shall be bound by secrecy or confidentiality** concerning the performance of his or her tasks, in accordance with Union or Member State law.'
Professional qualities	Art. 37(5)	'The data protection officer shall be designated on the basis of **professional qualities** and, in particular, **expert knowledge of data protection law and practices** and the ability to fulfill the tasks referred to in Article 39.'
	WP29	'Ability to fulfill the tasks incumbent on the DPO should be interpreted as **both referring to their personal qualities and knowledge, but also to their position within the organisation. Personal qualities should include for instance integrity and high professional ethics.'** 'The **necessary level of expert knowledge** should be determined according to the data processing operations carried out and the protection required for the personal data being processed. For example, where a data processing activity is particularly complex, or where a large amount of sensitive data is involved, the DPO may need a higher level of expertise and support. Relevant skills and expertise include: • **expertise in national and European data protection laws and practices** including an in-depth understanding of the GDPR • **understanding of the processing operations** carried out • **understanding of information technologies and data security** • **knowledge of the business sector and the organisation** • the **ability to promote a data protection** culture within the organisation.'

3/ WHAT'S NEW?

This section gives an overview of the main events within Ethikos during the past quarter.

a. MER Conference

In May 2020, Ethikos had the pleasure and honor to speak at the MER Conference 2020 about the enforcement of GDPR two years after its release.

Click here to watch our webinar (in French) based on the presentation given during the MER Conference.

b. The arrival of Nicolas Delvoie, our new Real Estate Partner

In June 2020, we were pleased to announce the arrival of a new Partner at Ethikos: Nicolas Delvoie, a recognized specialist in real estate and property law.

Click here to see the press release.

Click here to see Nicolas' full profile.

c. New website

In June 2020, Ethikos also launched the new version of its website, which is more complete and user-friendly.

One of the main novelties is the addition of a new page describing our innovative and flexible pricing packages as well as our 'Field Lawyers®' services.

The newsletter is published by the law firm Ethikos SRL with the collaboration of Thomas FAELLI - Frédéric DE CAMBRY - Miguel MAIRLOT - Pierre VAN SCHERPENZEEL - Nicolas DELVOIE. Layout: Mathieu RÜTIMANN. The information published by Ethikos SRL is for information purposes only. It does not constitute legal advice on specific situations. Reproduction is authorised, except for commercial purposes, provided the source is acknowledged. Responsible edito: Miguel Mairlot, Avenue Louise 200, 1050 Brussels, phone: +32 2 895.90.02; e-mail: m.mairlot@ethikos.be. If you received this newsletter by e-mail and you do not wish to receive it anymore, please send us an e-mail at info@ethikos.be.