

De la relation

DELSOL AVOCATS
LA QUALITÉ DE LA RELATION

#23 December 2020

The DELSOL Avocats
newsletter



Xavier DELSOL
Chairman
of the Board



Both the economic world and our everyday private lives are increasingly dependent on IT tools and new technologies, particularly as regards the circulation of information. But such a change always comes with new forms of fraud, such as «business email compromise» for example, and other kinds of cyber attacks.

We therefore thought it necessary to advise our clients on these cyber security issues to help them take preventive measures upstream or swiftly react if they are the unfortunate victim of such an attack. You will find all the aspects developed below in this Newsletter.

This new issue of our newsletter, still mainly emailed to our clients, is also an opportunity for us to welcome a 28th partner to the firm, Thomas AMICO, and his team, to strengthen our «Litigation» department, primarily in «White Collar Crime» and «Compliance». In this area too, common decency is no longer sufficient in the face of increasingly stringent transparency regulations and growing demand from consumers and business customers for principles and guarantees, even if they are not required by law.

Despite the difficult times we have all experienced in recent months, our firm has continued evolving, to stay on course and be available throughout the lockdown and home-working periods. There is no doubt that working from home and new videoconferencing technologies facilitated the application of health measures and, in some cases, even temporarily made working life easier and more comfortable. But they have also shown their limits and confirmed that nothing replaces, at least not as well, direct face-to-face contact and quality relationships, both among staff and with clients. They need to discuss their environment and their difficulties, projects and needs... so that we can provide the right solution. As is often the case, striking the balance will no doubt be the answer for the future.

Here at Delsol Avocats, we dearly hope that, despite the complex situation, the Christmas holidays will allow you all, our clients and readers of this newsletter, to prepare for a new year that we are convinced will bring renewed success.

A 28th partner at DELSOL Avocats: Thomas AMICO joins the «Litigation – White Collar Crime» department and creates the Compliance practice

Thomas AMICO joined the firm on 5 October as partner and co-head of the «Litigation – White Collar Crime» department alongside Alexis CHABERT, Pierre-Marie DURADE-REPLAT and Stéphane PERRIN.

This new arrival is an integral part of the firm's development strategy and completes our offering with a new Compliance practice.

Thomas AMICO brings the firm his expertise in white collar crime and compliance. His practice encompasses all violations of business law, from corruption to cybercrime, fraud and press offences. He regularly assists businesses and senior executives in criminal proceedings in France and abroad. For example, he represented the interests of the Republic of Senegal in the trial against the former mayor of Dakar, accused of embezzling public funds. He is currently defending one of the protagonists in the «Kazakhgate» affair and is also

counsel for the defence in an international trial concerning counterfeited luxury goods.

Thomas has also developed considerable expertise in compliance and risk prevention. He assists international groups on implementing compliance programmes to meet the requirements of France's Sapin 2 Act and due diligence law.

Admitted to the Paris Bar in 2009, he began his career at Veil Jourde (2009 – 2013) and later joined the French office of Linklaters, where he headed the Criminal Business Law and Compliance practice (2013 – 2020).



«Companies and their senior executives are increasingly facing criminal and compliance issues. Joining DELSOL Avocats enables me to provide assistance on these issues from an independent standpoint and to benefit from the multidisciplinary expertise of my colleagues on the cases we handle. I am looking forward to playing my part in developing a top-notch criminal business law and compliance practice», says Thomas AMICO.

CYBERSECURITY: an issue that calls for reflection... fast!

The Covid-19 epidemic and the development of home-working multiply vulnerabilities and prompt cybercriminals to take advantage of this unprecedented situation. Visits to the French government's cybersecurity support and prevention website «cybermalveillance.gouv.fr» have increased five-fold since the start of the epidemic.

Businesses face considerable consequences, given that 60% of SMEs file for bankruptcy within six months of falling victim to a cyber-attack. Now that this potential cyber risk has become a reality, what measures are companies taking to anticipate, act and manage these attacks?

Organisations must anticipate, act and respond

Anticipate by identifying the assets to protect and the potential threats (by several methods: EBIOS, impact assessments) and by defining a security policy adapted to the company's risks, raising employee awareness, and introducing internal policies and procedures covering all aspects of cybersecurity.

Organising specific governance within the company to deal with a crisis is also an important factor. Be it by the ExCo or a crisis management unit, directions must be given to marshal the required resources and organise communication.

The General Data Protection Regulation (GDPR) which came into force in May 2018 also reminds us that the Controller answers for any loss or theft of data entrusted to a processor. Contractual commitments must therefore be reinforced and risk-sharing organised, particularly by looking into the advisability of purchasing cyber insurance.

Act next, because it's no longer a question of whether a company will be attacked but when. Furthermore, in recent years, cybercrime has become more visible

than before, particularly with the development of ransomware.

In the event of a cyber-attack, the organisation should gather together as much evidence as possible, most of which will be digital. It should be collected by internal teams and specialised service providers, such as security audit or security incident detection service providers qualified by the French National Cybersecurity Agency (ANSSI).

Respond at the same time, by marshalling evidence necessary for the organisation to take action in response to cyber-attacks.

On a legal level, the company can lodge a complaint with the Public Prosecutor, by providing all the information and evidence in its possession. Secondly, as data controllers, companies must notify the data protection authority of any data breach within 72 hours of becoming aware of it, pursuant to Article 33 of the GDPR. When the data breach could create a high risk for the rights and freedoms of natural persons, the controller must also inform the data subject of the breach without delay.

In the event of loss or theft of personal data, a company may be fined up to 4% of its global annual revenue or €20 million.

Jeanne
BOSSI MALAFOSSE,
Partner, Head of
the «Personal Data»
department



Between February and March 2020, Interpol recorded a 569% increase in cyber-attacks (malware and phishing)¹.

In its information report no. 502 dated 10 June 2020 on cyber threats during the health crisis, the French Sénat found that «*cybercrime rises 10% per year*».

According to CNIL, «*Since the beginning of the year, ANSSI has handled 104 ransomware attacks*» and the authority itself received 2,287 notifications of data breaches in 2019.

¹ Source Webpage presenting the Interpol report dated 4 August 2020.

Business Email Compromise makes the most of the health crisis

We could all naively believe that we are protected from this type of fraud, no doubt the earliest of the cybercrime era. Yet, the global health crisis has revealed weaknesses in companies in countering this type of attack.

The past months have seen an alarming rise in this form of fraud, which costs French businesses millions of Euros each year. How can organisations avoid it when, with staff working from home, the same levels of control can be difficult to maintain?

First of all, let's look at how this simple and highly effective mechanism works.



Most obviously, the cyber criminal does not need to be a computer wizz. They simply need to make the company's employees or regular partners believe they are the CEO. To do that, they use fake email addresses almost identical to the organisation's official ones, but for a few letters. They then ask an accountant to make an urgent bank transfer for a secret deal. Otherwise, they might ask for a change of bank account before paying a real invoice.

There is almost always no accomplice inside the organisation. The staff therefore believe that the request comes from their boss and do not question the order they receive, either as a reflex or out of fear of their demands for an explanation being considered inappropriate.

Well-organised cyber criminals who know the company's internal organisation quite simply exploit the employees' lack of wariness and often, the absence of internal controls. It's important to note that, although they are at the forefront of these scams, banks are often negligent in implementing effective controls despite the strict obligations they must meet.

But counting solely on the staff being spontaneously cautious would be simplistic and ineffective, as this is often incompatible with their workload and working conditions. Not only should they regularly receive specific training, but double checks must be the rule.

First, any new bank details must be checked. Whatever the type of fraud, entering new bank details into the organisation's accounting system is a vital step. However, any payment made to an unknown bank account must be systematically checked, particularly if the account is foreign, as is almost always the case. This means researching legal information about the payee company using all available resources and cross-checking data to detect any inconsistencies (Google search, request for banking information, verification of phone numbers via different sources). Where information is not available or is inexplicably inconsistent, an internal procedure must result in blocking the payment.

In addition, the order received must always be checked with several people, including at least the person who has bank signing authority. Using the «reply» or «reply to all» email function must be banished when performing these controls. Emails should only be sent to pre-saved addresses. Companies should not hesitate to develop a stricter system of controls when the amount, payee or frequency of a transfer is suspicious. Remember that, depending on how a company generally pays transfers, the fraud can be committed either by several transfers for small amounts or one for a very high amount.

If these prior measures did not avoid the scam, then responsive action is required fast. The funds can still be frozen within 48 hours of the transfer at banks, particularly when they are based in Europe.

Thereafter, there is little chance of recovering the money and a complaint must be lodged. The investigations are long (several years) and are rarely successful. The company's only option is then to hold the bank liable, as they are often negligent in checking transfer orders they receive. This negligence is particularly serious as banks have specific obligations regarding

AML-CFT controls and much more effective verification means than their clients.

Alexis CHABERT
Partner, co-head of the
«Litigation» department

Cyber-Insurance

The recent period has shown that law firms are prime targets for hackers, just like any other business; but all the more so, because confidential client data transit via their information systems. DELSOL Avocats realised the importance of securing its IT system long ago and is equipped with the latest technologies to protect both the system and the data it contains (multi-layer verifications, anti-virus analysis, deep packet inspection and software restriction strategy, daily reconstruction of remote connection servers, data storage in a specific format, etc). Information system security accounts for around 9% of the firm's annual IT budget.

But even the very best protection will not stop the cyber-attack from happening. Out of constant concern to ensure the best possible protection for our clients' data, we have an insurance policy covering cyber-risks with HISCOX ASSURANCES, a leading market player.

To us, customer relationship quality must rhyme with security!

Stéphane PERRIN
Partner, co-head of the «Litigation» department

Covid-19 or the ransom of fear

The Covid-19 crisis has led to a multiplication of cyber-attacks, particularly attacks by ransomware. According to its latest figures, ANSSI had recorded almost 130 such attacks by 30 September 2020, compared to 54 in 2019.

Ransomware (also known as cryptolocker) is a type of malware that blocks the target's data by encrypting files saved in infected computers before demanding payment of a ransom in return for a decryption key. The health crisis was a particularly propitious time for ransomware attacks due to the stressful climate that tends to make us less cautious, and the rapid and extensive use of home-working with its ensuing security flaws. A whole host of fraudulent messages offer downloadable infected files, such as false travel exemption forms or fake forms for donating to charities or public organisations. Once the worm is in the apple as the French saying

goes, it spreads through the computer in next to no time and ends up completely paralyzing the target organisation.

France has a long list of ransomware victims including Orange, Saint-Gobain, Tarkett, M6, Fleury-Michon, Bouygues Construction, Eurofins and Altran, as well as hospitals, Ministries, law firms and town halls. Microsoft recently said they had detected attacks or attempted attacks on several laboratories «that have Covid-19 vaccines in various stages of clinical trials», which slowed down the trials and hence the release of the vaccines.

On 4 September 2020, ANSSI published its health protocol for

cyberspace in partnership with the French Ministry of Justice. This awareness guide for businesses, local authorities and administrations aims to instil barrier measures to protect against computer viruses and avoid their spread, particularly as regards ransomware. Ransomware attacks have various legal characterisations and the Public Prosecutor, the Investigation Section, the Criminal Court and the Assize Court in Paris have national jurisdiction for attacks on automated data processing systems and the fundamental

interests of the Nation, including ransomware. A division of the Public Prosecutor's department in Paris specialises in complex cybercrime and has solved several major cases, sometimes resulting in the arrest of accomplices within the target organisation.

Therefore, any company or organisation that falls victim to a cyberattack must gather and retain all the evidence to swiftly lodge a complaint and attempt to identify the criminals and any accomplices. Buying specific insurance can

also be a good idea and, in some cases, it will cover all or part of a ransom demanded to decrypt critical data and resume business. Lastly, it is sometimes possible to sue negligent or defaulting third parties to claim compensation for attacks suffered.

Combating cyberattacks is therefore more than just a technical issue; it must also be done on a legal level using the growing set of tools our law offers. Our firm has all the necessary expertise and experience to assist you and minimise the impact in the event of a cyberattack.

Unlawful Online Content: Fight, but safeguard freedom of expression

Digital fraud has many facets, ranging from ransomware that paralyzes a business, phishing for sensitive data, «business email compromise» aiming to convince an employee to urgently transfer money at the alleged request of the boss, or the sale of counterfeit goods on internet, including paper face masks and adulterated hand sanitizer which is totally ineffective against coronavirus.

Another form of cybercrime is also appearing recurrently, namely the posting of unlawful content on internet, and particularly on social media websites. Be it hate mongering, racist or anti-religious insults, slander or advocating

terrorism, these contents are multiplying and spreading at breakneck speed by being instantly passed on by millions of people. Recent news has unfortunately demonstrated the tragic consequences these posts can have.

France's 2004 law for building confidence in the digital economy (LCEN) establishes the principle that a social media website is only required to act if it becomes personally aware of the content or if the content is reported to it by a user via a very specific procedure. The website must then satisfy itself that the content is «manifestly unlawful» (i.e. in practice, terrorist, child pornographic or inciting racial hatred) and if it is, it must «promptly»



withdraw it. Otherwise, the matter may be referred to a judge who will order its withdrawal. The so-called «Avia» bill required online platform and search engine operators to withdraw any manifestly unlawful content, such as hate mongering or racist insults, within 24 hours after reports by one or more people. For terrorist and child pornography content, reported this time by the administrative authority, the deadline was reduced to an hour. But in a decision dated 18 June 2020, the French Constitutional Council censured these provisions

in the name of freedom of expression, noting, particularly, that an hour was not long enough to bring an effective appeal before a judge and, in respect of the 24-hour deadline, that the very broad scope of the law did not give the websites sufficient time to analyse and contextualise the reported content.

There is no doubt that the debate is not over. But the fact remains that appealing to the judicial authority currently offers the best guarantees. A judge is indeed in the best position to weigh up the

interests, censor unlawful content and punish the perpetrators for slander or insult for example, while safeguarding the fundamental democratic freedom of expression.

It is possible to fight against unlawful and malicious online content under current law and case law. Various solutions can be adopted but certain conditions must be met (deadlines, form, etc.) to guarantee freedom of expression that is so important in France. Our firm is here to help if you are the target of unlawful online posts, to initiate criminal or civil proceedings against the culprits or seek withdrawal of the content from the host websites.

Thomas AMICO
Partner, co-head of the
«Litigation» department

In the press...

DELSOL Avocats assisted Caisse des Dépôts et Consignations (CDC) with its acquisition, through Banque des Territoires, of a minority stake in the semi-public company (SOCOMIX) operating the Hôtel du Palais in Biarritz with a team comprising partner **Philippe MALIKIAN**, and associate **Alexia DEMONCHY** for corporate aspects; and partner **Julien MONSENEGO**, and associate **Clément GUITET** for tax aspects. La Lettre des Juristes d'Affaires and Le Monde du Droit reported on the deal.

Laurent BUTSTRAËN, partner, and **Anne-Sophie FRANC**, counsel in the «Non-Profit Organisations - Social Entrepreneurship» department advised Doctegestio, France's leading global healthcare and wellness operator, when it joined the governance bodies of Union Mutualiste pour la Gestion du Groupement Hospitalier Mutualiste de Grenoble (UMG-GHM) through its two mutual insurance companies. Juristes Associés reported on the deal.

DELSOL Avocats advised higher education group EDH on its acquisition of CREAD Institut with a team comprising **Henri-Louis DELSOL**, **Vincent GUEVENOUX** and **Alexia DEMONCHY** for «Corporate Law - Mergers & Acquisitions»; **Julien MONSENEGO** and **Clément GUITET** for «Tax law»; **Benoît BOUSSIER** and **Sarah FERRAD** for «Real Estate»; and finally, **Delphine BRETAGNOLLE** and **Jessica NEUFVILLE** for «Employment Law - Social Welfare law». Capital Finance, Le Monde du Droit and Juristes Associés reported on the deal.

Renaud-Jean CHAUSSADE, partner, and **Alexis ROBBE**, counsel, from the «Public Law» department wrote four articles published in La Gazette des Communes:

- «The obligations of municipalities with fewer than 5,000 inhabitants»,
- «Solutions in response to disturbance of the peace»,
- «The roles of inter-communal organisations» and
- «Accommodation obligations applicable to local authorities».



DELSOL Avocats advised Garibaldi Participations on its acquisition of an equity stake in Vacancéole. **Frédéric SUBRA** worked closely with Garibaldi Participations on the fiscal due diligence. Capital Finance reported on the deal.

DELSOL Avocats advised the Serge Ferrari Group on its acquisition of Verseidag-Indutex with a team consisting of **Emmanuel KAEPPELIN**, partner and co-head of the «Corporate Law - Mergers and Acquisitions» department, counsel **Raphaël ORY**, and associates **Caroline DA LAGE** and **Melanie DEBERNARDI**. Counsel **Séverine BRAVARD** and associate **Leslie d'ALASCIO** advised on matters relating to structured financing. The acquisition was handled in conjunction with German law firm BUSE HEBERER FROMM, a fellow-member of Telfa (the Trans-European Alliance of Law Firms). Le Monde du Droit reported on the deal.



Julien MONSENEGO wrote a contribution on the consequences of the Covid crisis on transfer pricing and international taxation in the Bloomberg Tax «Spring/Summer 2020 Transfer Pricing Forum» series.

DELSOL Avocats advised NEW MT, a company controlled by the historical shareholder of KING JOUET, in the context of its takeover offer over MAXI TOYS subject to judicial reorganization proceedings before Mons commercial Court (Belgium). The DELSOL Avocats team working on this deal consisted of: **Pierre GOUGÉ** and **Jean-Philippe DELSOL**, partners and co-heads of the «Corporate Law - Mergers and Acquisitions» department, **Manuel WINGERT**, Counsel specialised in insolvency proceedings, associates **Anaïs FAURY**, **Martin SOUYRI** and **Alexia DEMONCHY** and legal advisor **Edouard PIQUE**; Counsel **Séverine BRAVARD** and associate **Leslie d'ALASCIO** as regards funding; **Frédéric SUBRA**, Partner and co-head of the

«Tax Law» department and Counsel **Paul ALMEIDA**; **Delphine BRETAGNOLLE**, Partner and co-head of the «Employment law» department and counsel **Jessica NEUFVILLE**; **Stéphane PERRIN**, partner, for intellectual property aspects. La Lettre des Juristes d'Affaires, Fusions&Acquisitions Magazine and Le Monde du Droit reported on the deal.



Manuel WINGERT answered questions from Next Step together with Aurélie PERDEREAU (Thévenot Partners) in an interview entitled «Sortir de l'anesthésie des mesures étatiques avec confiance» (Confidently bring State measures out of anaesthesia).

Three new Counsels at DELSOL Avocats

DELSOL Avocats is delighted to announce the promotion to Counsel status of **Léa ZÉRILLI** in the «Tax» department and **Raphaël ORY** in the «Corporate law - Mergers and Acquisitions» department, and the arrival of Counsel **Cécile BUZY** who joins the «Employment law - Social welfare law» department.



Léa ZÉRILLI was admitted to the Paris bar in 2010 and joined DELSOL Avocats in 2015. She assists individuals and family groups in the context of restructuring transactions, asset transfers and optimizations in either a domestic or an international framework. She also works on the tax aspects pertaining to mergers & acquisitions transactions and on taxation disputes.



Raphaël ORY has developed expertise in corporate finance and transfers as well as in private equity and contractual restructuring (supply, manufacturing, consortium, etc.). He worked for five years in Asia within a leading French law firm and developed specific knowledge of cross-border transactions. He therefore assists both foreign groups in France and French groups abroad. **Raphaël ORY** was admitted to the Paris bar in 2009 and joined DELSOL Avocats in 2017.



Cécile BUZY, was admitted to the Paris bar in 2005 and joined DELSOL Avocats on 2 September 2020 after more than 13 years within a French full service law firm. She specializes in labour law and advises and conducts litigation for companies in the context of restructuring and transformation transactions. She also advises French and foreign companies on all aspects of employment law.

These appointments demonstrate the firm's ambition to continue training and promoting talent in-house. Our recruitment of new profiles also reflects the vitality of DELSOL Avocats.

Events

Throughout lockdown, we remained committed to keeping our clients informed by means of webinars, and we are continuing this process of providing information remotely:



Gilles VERMONT, Counsel in the «Litigation» department, ran a series of four videos focussing on compliance. The first episode was devoted to the Sapin II Act, the second to compliance litigation, the third to risk mapping and the last one to third-party evaluation. These videos are available on the firm's website and LinkedIn page.

She co-led the roundtable discussion on «Monitoring employee activity».

03/12/2020
«Research: the advantage of distinguishing sample series in collections of human biological samples!», a webinar led by **Thomas ROCHE**.



19/11/2020
Jeanne BOSSI MALAFOSSE took part in the 3 Sphères e-health symposium organised by Docaposte, an affiliate of La Poste, in partnership with Le Point. She participated in the roundtable discussion on «e-health, for better ... not for worse».

8/12/2020
Thomas ROCHE took part in TIPS in the conference on «Clinical trials: managing studies during the pandemic».

04/12/2020
Elsa LEDERLIN took part in the symposium organised remotely by AFDI, ENM, INTEFP and the Cour de Cassation on «The employer's management power during the Covid pandemic».

03 et 10/11/2020
«Flash audit at the beginning of a term of office»: webinars by **Renaud-Jean CHAUSSADE** and Jean-Christophe

CARREL, Public Accountant in charge of the public sector, Acticonseil - Training for local authorities.

05/11/20
«Adaptation measures to cope with the current crisis: where do we stand»: a webinar led by **Philippe PACOTTE** and **Stéphane HENRY**, Public Accountant - Statutory Auditor, partner in the firm EUREDIT

16/10/2020
«IT contract drafting: vital clauses and negotiating levers»: a webinar led by **Jeanne BOSSI MALAFOSSE** and **Caroline CHANCÉ**.

23/09/2020
«Working from Home»: should we continue the positive experience of lockdown?» led by **Camille ROUSSET**, in partnership with **Laurène REGOUT**, corporate coach, and **Christophe JAOUEN**, associate director of the strategy management consultancy A Sens Ouvert.

FONDS DE DOTATION

DELSOL AVOCATS
LA QUALITÉ DE LA RELATION

DELSOL Avocats Endowment Fund annual competition: And the winners are ...

For the 11th year in succession, DELSOL Avocats organised a call for projects to select the winners of its endowment fund awards and, for the first time, a remote prize-giving event was held on 4 November 2020.

The three finalists were asked to present their organisation and project in the form of a 10-minute video, to inform and convince the panel of judges.

During the deliberations, the winners and other connected participants were given advice by **Laurène HERBELIN** from the fundraising specialist Philanthrôpia.

The first prize of €20,000 was awarded to **Solenciel**, an organisation giving young women the opportunity to leave the world of prostitution by offering occupational training followed by a permanent employment contract in professional cleaning services. Solenciel also provides comprehensive support for real integration into society.

The second prize of €10,000 was awarded to **Visitatio** which takes innovative action based on local mobilisation to provide companionship for dying patients at home and support for their carers.

The third prize of €5,000 was awarded to **La ligne vertueuse** which gives young adults facing failure an opportunity to gain experience in a company, to produce, mount and assemble furniture made from unused discarded materials.

DELSOL Avocats Endowment Fund is delighted to offer its support to these three organisations and thus help them pursue their development.

Lawyer Initiative



To assist our clients facing international concerns, DELSOL Avocats is a member of TELFA (Trans-European Law Firm Alliance), a network bringing together over 1,000 lawyers in Europe as well as professionals from its American counterpart, USLAW.

Early in 2020, **Eve DAUVOIS**, associate in the «Tax law» department, took part in a six-week exchange programme in Milan, with tax lawyers from the firm Legatitax.

In addition to enabling lawyers to improve their language skills, this kind of experience opens up their horizons and gives them a better understanding of international affairs and the specific features of each country. Given the growth of internal trade, relationships with foreign law firms must be strengthened. We therefore hope to see similar initiatives develop in future!



17/09/2020
Anti-gift law: applying the thresholds laid down by the orders of 7 August 2020: a webinar led by **Thomas ROCHE**.



15/09/2020
«Home-working: an employee right and/or a form of organisation for the employer?»: a webinar led by **Elsa LEDERLIN**, in partnership with **Jean-Pierre GASPARD**, Director of IDAF (ex-Director General of AFMTéléthon) and **Philip MODOLO**, voluntary elected Secretary General, Les Restos du Coeur.