



PERSONAL DATA “APPOINTING PRIVACY OFFICER WAS THE RIGHT DECISION FOR US”

When it comes to personal data protection, the law alone is not enough. The “CNIL Registered Data Protection Officer” (Privacy Officer) function - along with the soon-to-be-instituted Data Protection Officer (DPO) is a key component of regulating through practice.

In this time of regulatory change and as risks connected with data processing grow, many company leaders have chosen to appoint a Privacy Officer: **ten of them share their story here.**



GMF : DATA, A CORE BUSINESS ASSET

For an insurance company like GMF, data are a vital asset, especially looking ahead to the day when all data managed will come from connected objects. This is why the CNIL Registered Data Protection Officer function is so important.



“
DATA ARE A FORM
OF WEALTH AND ARE
AT THE HEAR OF ALL
OUR PROCESSES.
THEIR QUALITY
AND RELIABILITY
ESSENTIAL TO US;
AND WITH BIG DATA,
THEY ARE EVEN
MORE SO”

Laurent TOLLIÉ
Managing Director

GMF Assurances serves 3.5 million policyholders, employs 5,000 men and women, and provides insurance for 3.1 million cars and 2.7 million homes. The company is a subsidiary of COVEA (€16.5 billion in turnover, 11 million policyholders, 25,000 employees), which also includes companies such as MAAF, MMA and GMF.

In the splendid hewn-stone building that was previously home to the Head Office of Chemins de Fer de l'Ouest, near Paris Saint-Lazare Rail Station, Laurent TOLLIÉ, Managing Director of GMF Assurances, makes no secret of how important personal data are to his business: “They are a source of wealth and are at the heart of all our processes. Their quality and reliability matter tremendously to us. With Big Data on the horizon, they will be even more important.” “Precisely because of their profession, insurance providers process more personal data than almost any other business player”, explains Alexandre Eloy, Privacy Officer at GMF Assurances, “and as a result, we have to show the utmost stringency.”

Laurent TOLLIÉ does not side-step the questions that come to mind when addressing an insurance provider about the explosion of connected objects.

“When will insurance premiums be indexed on heart rate, based on the data gathered via fitness wristband?” GMF Assurances’ Managing Director took on the tricky question: “Clearly, that is one possible way forward for our business sector. Working with data from connected devices, we will be able to customise our insurance offer, come up with innovative services and develop new and more effective prevention tools. However, we also need regulations, rules and ethics, in order to identify the lines not to cross”.

Questions like these highlight just how crucial the CNIL Registered Data Protection Officer is at a company like GMF Assurances. “Take the example of data from a connected car”, explains Alexandre Eloy, “We will need to answer many new questions. Who will have control of the data: the manufacturer, the buyer or the insurer? What will we be entitled to do?” In the opinion of GMF Assurances’ Privacy Officer, “The future is taking shape now and the Privacy Officer will have a central role in it. I am definitely one of the people who have a finger on the company’s pulse, innovation and dynamism, and who reports these aspects back to top management”.

Alexandre Eloy, like his counterparts at MAAF and MMA, works daily to ensure compliance with regulations, and not only those specific to the insurance sector. He is also watchful over the impacts of new issues brought about by technological progress. GMF’s Privacy Officer is furthermore responsible for liaising with CNIL. “We worked in close conjunction to develop the ‘compliance pack’ which the Commission designed specially for us in the insurance industry. Thanks to that legislation, we were able to determine a more operational framework to take into account the new media, such as Internet or the social networks.”

“Actually,” continues Laurent TOLLIÉ, “the function of the Privacy Officer is at the crossroads between three dimensions: a technological dimension, an insurance dimension – sizing up risk -, and a regulatory and ethical dimension. It helps me determine the framework by which a company like ours will abide. I also expect my Privacy Officer to make the topic of Data Protection an important one for all our business lines, and that this aspect is taken into account upstream in all of our projects, when they are still in the development stage”.

For all of those reasons, the Privacy Officer has a reporting line that enables him to conduct his action (he reports directly to the Secretary General) and works full-time on Privacy Officer responsibilities (even supported by another person). As to the action run by the Privacy Officer, appointed in 2014, the bottom line is clearly positive: “The Privacy Officer makes it possible for us to take personal data issues into account upstream and provide more security on those compliance aspects. Last but not least, for a company like ours, it is also a matter of image and trust for our policyholders”, concludes Laurent TOLLIÉ.

PEOPLE: THE BEATING HEART OF ASSOCIATION DES PARALYSÉS DE FRANCE

For Association des Paralysés de France, personal data protection is an imperative – as the association illustrated by appointing a CNIL Registered Data Protection Officer in 2010.



“ THE PRIVACY OFFICER SERVES AS WATCHGUARD AND STIMULUS. HE IS A FACILITATOR, A MESSENGER.”

Prosper TEBOUL
Director General

Association des Paralysés de France (AFP) was founded in 1933, at the impetus of four determined young people, stricken by polio and indignant at the exclusion to which they were victim. A non-profit association recognised of public benefit, APF is a national associative protecting and advocating for the rights of individuals afflicted by motor deficiencies or multiple disabilities, thanks to a budget of €750 million, 400,000 donors, 30,000 people under care, 26,000 members and 14,000 employees.

For Prosper Teboul, Director General of Association des Paralysés de France, protecting personal data is a matter of course, considering the values advocated by APF, including respect for the fundamental rights of individuals and

in particular to privacy: “*The Charter Committee makes the Data Protection Act an essential watchpoint.*» *Our 400,000 donors need to be aware that we take the utmost care of the data they entrust to us. A database like ours can be very valuable to some. To mitigate that risk, we chose to outsource data processing to a specialised service provider, which guarantees us maximum security -- in addition to this, we run our own verifications*”.

In order to better serve those who come to it for assistance, the association is rolling out a database system designed to accommodate unique digital records for all users across all 500 of its medical-social services and establishments.

The aim is to enable the support team’s professionals to share information in a secure environment. In order to ensure compliant data processing and data security, the base was entrusted to a healthcare data hosting provider, accredited by ASIP Santé: “*It is our duty to secure our data as much as possible*”, stressed Prosper Teboul, “*the institution’s image and credibility depend on it*”.

For that reason, the CNIL Registered Data Protection Officer, Abdou-Issa Papa, officially appointed for CNIL affairs in 2010, reports directly to him. Already in charge of compliance in data processing with respect to the Data Protection Act, as implemented by the APF several years ago, Mr Papa completed a long-term degree programme in 2012, the Master’s Degree specialised in Personal Data Protection and Management at ISEP, funded by its employer. One of his first decisions was to overhaul the IT Systems User’s Charter, an appendix to the Internal By-Laws. He has the resources needed to do so, first and foremost, an adjusted workload plan, under which he was able to run awareness-raising that reached the vast majority of directors at the 500 structures and coordinate a community within the company’s social network.

Looking back at the work accomplished by the CNIL Registered Data Protection Officer, there is no doubt that the appointment was the right decision: “*He serves as a watchman, a stimulator*”, explained Prosper Teboul, “*He is a facilitator and a messenger. In one year’s time, he managed to identify one hundred Data Protection reference people in our structures. That feat very aptly illustrates his qualities as a coordinator and instructor*”.

Association des Paralysés de France’s Director General also points out that, “*the Privacy Officer encourages network-based operation and project-mode management in which all the teams to work together. It is similar to a quality assurance effort*”. In Prosper Teboul’s view, appointing a CNIL Registered Data Protection Officer “*is part of the duty to prevent*”, which befalls all company leaders.

“CUSTOMER DATA ARE A FORMIDABLE ASSET: PROTECTING THEM IS AN OBVIOUS IMPERATIVE”

Argosyn Group is dedicated to managing financial operations such as collection of receivables (Contentia), insurance brokerage (Direxi) and financial lending services (Cofidis Participation), while 3SI Group manages e-commerce operations and services to e-commerce companies, such as 3 Suisses, Blancheporte or Dispéo.



“ APPOINTING AN PRIVACY OFFICER IS A POWERFUL ACT THAT TELLS OF A COMPANY THAT RESPECTS ITS CLIENTS ”

**Stéphane
CHAMPETIER DE RIBES**
Secretary General

Argosyn Group employs 1,200 people in France, Spain and Luxembourg, and earns €400 million in sales revenue. As to 3SI Group, it receives twenty million unique hits to its Web site each month, in Europe. It is also the leading private provider of services to e-commerce companies in France, with over 6,000 e-merchants served in France, Belgium and Spain. It posts €900M in sales revenue, has 4,900 employees and nineteen active stores in twenty countries. 3SI is a 100%-owned member of the German corporation Otto, the World No. 2 in retail e-commerce.

In this renovated building in the suburbs of Lille, in Villeneuve d'Ascq, Stéphane Champetier de Ribes, Secretary General of Argosyn Group and Michel Rime, CNIL Registered Data Protection Officer, are all ears. The decision to appoint a CNIL Registered Data Protection Officer, already a few years ago, came as a matter of course.

It was not so much the German influence that swayed the Group, explains Stéphane Champetier de Ribes with a smile, though the function *Datenschutzbeauftragter* (literally, “person in charge of data protection”) has been in existence in that country since the 1970s: “Of course, our German shareholders had already appointed someone to handle data protection aspects -- as is required of them by German law -- but that was not what drove us. We felt it was important to appoint a CNIL Registered Data Protection Officer, from as early as 2007, though it was in no way mandatory”.

The reasons appear obvious enough: the personal data processed by the two Groups, including those regarding credit up to 2008, are ultra-sensitive. “There is a specific regulation on credit, which makes personal data protection for contracting parties a key part of the picture”, pointed out Stéphane Champetier de Ribes. “Moreover, for Groups like

ours, client data are a considerable asset: protecting them is quite naturally an imperative. Lastly, from as early as 2007, we had a feeling that the topic of personal data protection would become a major topic for countries and companies overall”.

The Group appointed a part-time Privacy Officer from that very year. Then, Michel Rime was appointed CNIL Registered Data Protection Officer on a full-time basis. With an insider's understanding of the Group thanks to his time at 3 Suisses' procurement centre, he knew each of its building blocks (Logistics, Marketing, Customer Relations, Human Resources, Procurement, etc.) and soon became a uniting force. In the eyes of Stéphane Champetier de Ribes, to whom he reports directly, the CNIL Registered Data Protection Officer is a “*watchguard*”.

That inside-out knowledge made it possible for Michel Rime to quickly set up and coordinate a network of some twenty intermediaries within the Groups' companies, which he brings together at least twice each year. As Stéphane Champetier de Ribes sees it, having a coordinator for the network of correspondents is essential for organisations working in areas as widely-varied and as much in contact with the public. True to the role of a “personal data” project head, he supervises, coordinates, advises and alerts the Management teams whenever circumstances require.

Stéphane Champetier de Ribes sums up his organisation's Privacy Officer experience as positive: “Of course, we could see it as a constraint -- but we were determined to turn it into an opportunity. For us, it is first of all an asset for our business: appointing a CNIL Registered Data Protection Officer is a powerful act that tells of a company that respects its customers, and makes it more attractive”, on a competitive market.

However, there is probably more it can do: the Secretary General of Argosyn Group has some advice for any organisations that might still be hesitating about appointing a Privacy Officer: “You have to make sure there is an appropriate and unchallengeable reporting line. The Privacy Officer needs to be positioned in such a way that he or she can assert that an act on the company's' part, regardless of the department in which it originates, might not be appropriate. That is one of the main reasons for which Michel Rime reports directly to me”, he specified.

WITH A PRIVACY OFFICER, WE ENJOY PEACE OF MIND

At the Local Council of Charente-Maritime, appointing a CNIL Registered Data Protection Officer brought more «peace of mind» to the Managing Director in charge of Services.



“ IT IS OUR RESPONSIBILITY TO PROTECT THE DATA PROVIDED TO US IN ALL CONFIDENCE BY USERS OF OUR SERVICES ”

Serge GAPAIL
Director General in charge
of Services

The Local Council of Charente-Maritime manages a large amount of personal data: those of its 3,000 civil servants, of course, but also and most importantly, that of its 648,000 constituents: “We manage the data on which individual solidarity benefits are computed, the information used to determine eligibility for Active Solidarity Income, as well as the personal data on school transport for 26,000 students, disabilities, benefits for new mothers and infants, etc. -- not to mention those connected with frequent user transport cards, to take the bridge over to Ile de Ré, and those connected with academic scholarships for future doctors whom we want to encourage to stay in the area. Overall, we track 51 lower secondary-schools”, specified Serge Gapail, Director General in charge of Services.

While some data is of obviously sensitive nature, like those relating to disabilities or to eligibility for Minimum Solidarity benefits, it quickly become clear that most of the data managed by the Charente-Maritime Council can prove critical. “It is our responsibility to protect the data provided to us in all confidence by users of our services”, Serge Gapail shares, “we need to respect that confidentiality and not break the bond of trust with the citizens”.

“Our greatest fear when it comes to the personal data entrusted to us is information theft, which would also carry a negative impact for our image”, added Serge Gapail. It is for that reason that a CNIL Registered Data Protection Officer, Marie-Laure Baron was appointed to the CNIL in 2014 by the Chairman of the Local Council, Dominique Bussereau.

“We already had a person in charge of access to administrative documents”, declared with the CADA, added Serge Gapail, “but Marie-Laure Baron’s role goes much further”. Reporting directly to the Director General in charge of Services in her function as Privacy Officer, to which she dedicates 80% of her time (the remaining 20% are set aside for coordinating IT skills network activities), she is vested with a three-fold mission, as Serge Gapail describes.

The first consists of spreading a real data protection culture across the local community. This means holding awareness-raising sessions with the departments, conducting poster campaigns, or running the Data Protection space on the Charente-Maritimes Intranet. “She also has to make sure that all the processes initiated are recognised and recorded in the local government registry, and when they are more sensitive, that they have been authorised by the CNIL”, specifies Serge Gapail, “because we want to prevent situations in which civil servants create records individually, without declaring them, for instance, and away from any supervision”. Marie-Laure Baron is also alongside all the project teams, from the incipient stages, and ensures that the processes initiated are compliant with the Data Protection Act. She has no qualms about alerting and advising the processes manager when relevant. “The decision to have the Privacy Officer report to the Director General in charge of Services shows how strongly committed Charente-Maritime is to data protection. It gives me real visibility and credibility. While I go about my everyday responsibilities independently, I know that Mr Gapail is always there to support and listen if I need it.

That synergy has made it possible for us to provide awareness-raising to over 1,000 local government workers about personal data protection and initiate compliance procedures on certain processes.”

As Serge Gapail says with a touch of humour, “Though I am a lawyer by training, my responsibilities as DGS don’t leave me much time to keep up with all the legal aspects around data creation and management. Marie-Laure Baron brings us true peace of mind”.

NEOTOA : A PRIVACY OFFICER TO ENSURE ETHICAL PRACTICE

For this property management company, which handles personal data on 18,000 lessees and 150 new owners each year, compliance in personal data processing is of the essence.



“
OUR PRIVACY
OFFICER ACCULTURED
THE ENTIRE STAFF TO
DATA PROTECTION
ACT COMPLIANCE
ISSUES;
IT DEMONSTRATES
OUR RESPECT
FOR ETHICS,
WHICH, FOR AN
ORGANISATION LIKE
OURS, IS EXTREMELY
IMPORTANT”

Bruno CACCIA
Managing Director

Founded as the “Ille-et-Vilaine Public Office for Low-Cost Housing” in 1921, then renamed OPHLM in 1950, and known up to 2014 as Habitat 35, real estate property manager NEOTOA employs a team of 200. Each year, it manages 300 transfers, allocates 2,500 housing units, sells 150 new homes and apartments to new owners, and fields 130,000 telephone calls to its call centre.

“NEOTOA, a property manager in Ille-et-Vilaine, has to keep up with growing demand for real estate. Each year, nearly 11,000 people choose to make their homes here”, explains Bruno Caccia, Director General of NEOTOA. “Some of the personal data we process are sensitive. Every day, we have to address conflicts between neighbours, overdue payments and property deterioration. Yet we are also considered a public service and have the duty to be exemplary”.

Any indiscretion could hurt such an organisation’s reputation. «We cannot let the trust relationship be harmed», says Bruno Caccia, summing up the core challenge. “Public opinion is increasingly sensitive to personal data gathering and processing: a single slip-up in the system and a whisper in the press can really impact us, in particular in terms of image”.

After the reorganisation run in 2010, NEOTOA found itself equipped with a new customer relationship centre. Within that new setting, the appointment of a Privacy Officer was a natural step. “After some consideration, we chose our Quality Manager, Isabelle Charpentier, who had initiated and largely contributed to the thinking behind the project”. Wearing “two hats” offers many benefits, as compliance and quality process inspections are closely intertwined in any company.

Working in conjunction with its Privacy Officer, NEOTOA’s Management team set out multiple responsibilities: The Privacy Officer must enable acculturation through awareness-raising, calling upon employees in-house to take action. “We watch how our employees fill out records and conduct prevention and awareness-raising with them, rather than inspection. The role of the Privacy Officer is also to set up debriefing mechanisms and make all employees responsible for personal data processing, each at their own level. Our goal is to have ethics be a shared aim for all employees”, explained Bruno Caccia. «Following a period of ownership-building, the employees know what they are allowed to write in the comments areas on the lessee or owner records -- and what is prohibited», explains Isabelle Charpentier, who adds that “being Privacy Officer means being responsible and showing what works... as well as what doesn’t. There is a mutual trust relationship with the data processing manager, who can count on me to manage ‘CNIL Risk’, and we discuss openly about possible avenues for action, based on needs”.

To share best practices, Isabelle Charpentier readily worked with other DPOs appointed at other property managers. This approach is often mentioned by DPOs across all business sectors as a means of enjoying the benefits of shared experience.

Bruno Caccia’s sums up the experience as very positive: “Appointing a Privacy Officer made it possible to acculturate the company as a whole to Data Protection compliance”, he explains. “It demonstrates our respect for ethics, which, for an organisation like ours, is extremely important.”

Photo Credit : C. Ablain

RANDSTAD FRANCE: MATURITY IN PERSONAL DATA PROTECTION IS A REAL DIFFERENTIATING FACTOR

For a group like Randstad, which has made skills management the centre-pin of its business, personal data management and protection is an imperative, hence its pioneering decision to appoint a Data Protection Officer from as early as 2006.



“
OUR PRIVACY
OFFICER’S
SUGGESTIONS
BRING CLEAR
ADDED VALUE TO
WHAT WE DO”

François BÉHAREL
Group Chairman
Randstad France

Serving 50,000 customer companies, the human resources services company Randstad employs 58,000 interim workers per day, in full-time equivalent, and earns \$2.73 billion in sales revenue. In 2014, it assigned 1,800,000 jobs. “Our Group manages millions of personal data: those of our job-seekers, of course, but also those of our own employees”, explains François Béharel, Chairman of Randstad France Group. “These human resources data are our core business and form a legacy which we must preserve and promote”. This applies all the more as the Group has just rolled out on an ambitious Big Data policy, aimed at helping the labour market run more smoothly and improving its range of offering along the way. “In September 2015, we came out with a unique solution, based on a Big Data approach. It is a full-fledged decision-making tool for companies, job-seekers and public institutions”. The skills mapping solution addresses a specific need expressed on a given employment pool. For instance,

a company wishing to establish itself on a given territory will know whether the required skills are available locally, while those looking for a job will be offered a list of jobs based not on their original professions, but on a community of skills that can be transferred to another job. This is a Big Data solution based on the compilation of an internal reference base of 1,000 qualifications, 11,000 skills and an anonymised database of over 3 million résumés. “You can see why it’s so important for us to protect that know-how!” specified François Béharel.

He adds, “Big Data, just like Open Data incidentally, is one of the greatest challenges of our time. Our Privacy Officer makes recommendations upstream from any project including personal data processing. I expect the person to actively contribute to achieving the right balance between

four dimensions: innovation, business focus, respect for individual rights, and information security”, specified François Béharel. “While the Privacy Officer is first and foremost responsible for ensuring that the fundamental right to data protection is safeguarded, the cross-cutting approach taken, questions raised and suggestions bring clear added value to our projects, regardless of their nature”, pointed out the Chairman of Randstad France. “We operate in all areas of activity and, thus, directly or indirectly, the Privacy Officer may end up dealing with topics as diverse as the ban on social security data disclosure to intermediaries, geo-location, biometrics or comments zone management”.

The Group appointed a Privacy Officer from as early as 2006. He is neither a lawyer nor an IT specialist, and instead the Head of Audit and Internal Control. François Béharel was quick to add: “She reports to me directly and enjoys a great deal of freedom in decision-making. Her role and understanding of the processes are recognised across the Group”. She is assisted by a legal specialist and works in close conjunction with all stakeholders: the Legal Department, IT, Human Resources, Marketing Finance, Communication and Training, as well as with the Privacy Officer appointed at the Randstad Holding level. “The teamwork makes a big difference”, François Béharel emphasises.

“Beyond the responsibilities traditional to the Privacy Officer role, I see two challenges on the horizon”, he adds, “managing risks connected with compliance and personal data securisation, and improving governance. Furthermore, we need to continue paving the way for the future European Regulation, all the while keeping an ear open to the operational teams, in an environment where, due to digitalisation, the issues at stake and risks are only growing. That’s why it is important to work in stages, and in a spirit of continuing improvement”. Marie Eymond, the Privacy Officer at Randstad France, sees it just the same way: “Gearing up for the European Regulation is a fine challenge that will require us to review all our tools and governance for personal data protection in the organisations. In running this process, the Privacy Officer serves as the ad hoc compliance officer, working in partnership with all the stakeholders. We will need to put a lot of energy into it, but personally, this is a process I am looking forward to with great enthusiasm!” she confides.

All in all, François Béharel is very satisfied with the decision, adding nonetheless that some of the initiatives undertaken deserve to be better publicised: “We need to shine more of the spotlight on our maturity when it comes to personal data protection, as it is a real differentiating factor”.

AT CNAF, THE PRIVACY OFFICER IS A “GUARDIAN ANGEL”

In his office overlooking Parc Montsouris, Daniel Lenoir, Managing Director of *Caisse nationale des Allocations familiales* (the National Family Benefits Fund) and an advocate of the Data Protection Act from its very inception, emphasises the key part played by the Data Protection Officer in this branch of social security.



“ THE PRIVACY OFFICER PROVIDES US SUPPORT IN THE MODERNISATION AND DIGITAL TRANSFORMATION PROCESSES ”

Daniel LENOIR
Managing Director
National Family Benefits Office

At the head of the Families branch network, he oversees 102 Family Subsidies Offices, providing to support to 31.2 million people every day. In 2014, it paid out no less than €85.1 billion, in three main areas: family support, housing assistance, and solidarity benefits -- including Active Solidarity Income and the Disabled Adult Allowance.

As Marie-Noëlle Séhabiague, CNIL Registered Data Protection Officer at CNAF and Director of Macssi (Task Force on Audit, Data Protection Compliance and IT Security), the data vital to the Branch's responsibilities can truly be described as immaterial wealth: *“Families confide in us, they inform us of their social situation, and tell us about their difficulties and the unpleasant events which they come up against in life”*. Such a blessing calls for extra care: it is easy enough to imagine how avidly some might attempt to gain control of this most sensitive data.

Ethics is a value immediately raised by Daniel Lenoir: the CNAF needs to be flawless when it comes to compliance and protection of the personal data entrusted to it, not only with respect to its

duties, but also to protect its credibility. Particular attention is paid to how data are used and to compliance with professional secrecy rules required of the Branch's 35,000 civil servants.

It is a responsibility of which the CNAF's Managing Director is well-aware, being in charge of data processing at the national level. In Daniel Lenoir's opinion, data protection - and, consequently, security - are vital issues.

“It is my top concern. As with any complex IT system, there is a real risk of intrusion: being in charge of processing, I am acutely aware of the level of risk involved”. Furthermore, the Families Branch has ordered the closure of any Web sites connected with phishing campaigns that subvert the visual identity of the CAF in an attempt to deceive users. The CNAF regularly files complaints further to such campaigns.

The Managing Director also underscored the arrival of these modern-day “Big Brothers”. Claims due to terrorism are also an important topic to him.

As Daniel Lenoir sees it, the role of the Data Protection is key: *“That is why the CNAF appointed one from as early as 2009. She makes it possible for us not only to fulfil our requirements in terms of ethics, compliance and security, but also to manage the modernisation process”*, he specifies. CNAF, as part of its digital transformation process, has rolled out a customised, paper-free services offering that gives beneficiaries the chance to receive the best possible response to their expectations, in line with the “caring pathway” principle adopted. In addition, in order to fight deprivation of rights and open up new doors, the Branch held its first Hackathon in October 2015, where compliance was guaranteed by Macssi. Lastly, the provision of data in the Branch's Open Data area was intentionally slowed down in order to guarantee the necessary confidentiality and security for data. This just goes to show the importance which Daniel Lenoir places on data protection.

For all the aforementioned reasons, Marie-Noëlle Séhabiague, the CNAF's Privacy Officer, reports directly to the Managing Director and is independent from the IT Department. The expert spontaneously describes her role as that of a “guardian angel”, operating in a fully-independent manner and advises the head of data processing on these clearly thorny issues: *“For the Families branch, compliance with the Data Protection Act and data protection itself are of the utmost importance. They are what holds together the virtuous circle we have developed with our beneficiaries, interlaced by the personalised offers we develop and the trust they place in us. And for an organisation like CNAF, the guarantee of trustworthiness they provide is vital.”*

THE UNIVERSITY OF CORSICA: AWARENESS-RAISING AND EMPOWERMENT ARE THE TOP PRIORITIES

As Paul-Marie Romani, Dean of the University of Corsica, describes it, the Privacy Officer contributes to enforcing the National Information Systems Security Policy (PSSIE) and facilitates compliance-related action.



“IT IS MY DUTY TO PROTECT OUR SCIENTIFIC CULTURE AND INTELLECTUAL HERITAGE”

Paul-Marie ROMANI
Dean, University of Corsica

The Pasquale Paoli University of Corsica was founded in 1975 and opened in 1981. In the field of research, three R&D platforms have since sprouted there, and operate in partnership with major research bodies and industrial corporations: Myrte and Paglia Orba, for research on renewable energies; and Stella Mare, for fish resources. In addition, the University of Corsica is a member of the only Trans-National Hub for Research and Higher Learning - “PRES - Euro-Mediterranean ARC” - to which the Universities of Nice-Sophia Antipolis, Sud Toulon Var, Paris-VI, Genoa, Torino and Pisa belong.

Based on Corte, it is home to 4,500 students hailing from fifty different nationalities and works in conjunction with some 100 partner universities across the world. In addition to personal data on students and alumni, it is responsible for data regarding research projects, some of which are CNRS-certified. Given that environment, the decision to appoint a CNIL Registered Data Protection Officer

was a matter of course, for Dean Paul-Marie Romani.

“Our Privacy Officer, Pascale Urbani, was appointed in 2008, shortly after the function was created”, he explains, “His role goes well beyond stream-lining reporting procedures to the CNIL. It was essential, for instance, that we be fully compliant

with the policy on information systems established at the national level”.

For the Pasquale Paoli University and its Dean, data security, in particular when it comes to data from research, is an imperative. “We have been the target of multiple virus and hacking attacks. It is my duty to protect our scientific culture and intellectual heritage”.

Pascale Urbani’s role does not stop at compliance with the Data Protection Act, PSSIE or even protection for research data. She is also in charge of awareness-raising for University staff, Paul-Marie Romani describing the Data Protection culture as “fundamental”: “There is a tremendous amount of work to do on awareness-raising and empowerment here. To illustrate, our Privacy Officer took part in drawing up our IT Charter”.

Overall, impressions are positive: “Having appointed a Privacy Officer gives us a certain peace of mind. We are sure that we have fulfilled our obligations, protecting personal data and our immaterial assets, as well opening eyes to the issues at the University of Corsica”, asserts Paul-Marie Romani.

THE LILLE UNIVERSITY HOSPITAL AND RESEARCH COMPLEX

“COMPLIANCE WITH THE DATA PROTECTION ACT SHOULD NOT BE AN ADJUSTMENT VARIABLE”

For a hospital the size of ours - which handles 200,000 hospitalisations per year - personal data protection is a central challenge and data security a fundamental concern.



“THE DPO HAS EVERY REASON TO BE IN AN ESTABLISHMENT LIKE OURS”

Bruno DONIUS
Deputy Managing Director
THE LILLE UNIVERSITY HOSPITAL
AND RESEARCH COMPLEX

With an outstanding team of 15,000 healthcare professionals to its name, the hospital complex is the Lille Region's leading employer. Posting nearly 200,000 hospitalisations and 1,500,000 consultations per year, the CHRU (Centre Hospitalier Régional Universitaire) manages personal health-related data for nearly two million people, or half of the Nord Pas-de-Calais Region's population. No need to specify that there is no room for error when it comes to patient data protection.

“One of our key responsibilities is to guarantee patients that their personal data are secure at all times. It is of the essence that we prevent information leaks”, affirms Bruno Donius by way of introduction. “This is particularly critical considering the fact that, in 2014, in the United States alone, 4,500,000 patients are reported to have had their healthcare data stolen”.

Personal patient data is sensitive data, and protecting it is of vital importance. It is for this reason that, from as early

as 2008, Bruno Donius asked Guillaume Deraedt, already CISO at the CHRU, if he would be willing to also serve as CNIL Registered Data Protection Officer. Entrusting that strategic position to a security expert, fully aware of the risks and issues at stake, is no light decision and shows the importance which the establishment places on protecting information. “Data security cannot be seen as an adjustment variable in the hospital's budget”, said the Deputy Managing Director pointedly.

The hospital being a world all its own, the Privacy Officer has to “juggle” with the imperatives of doctors' and care providers' professions. For instance, in some cases, doctors and surgeons need to be able to very quickly access a patient's personal data, in particular in the event of an

emergency operation -- a situation which requires, in hospital lingo, going into «icebreaker» mode. At such a crucial point in a patient's life, data protection naturally gives way to data accessibility and integrity, as provided for moreover by the Data Protection Act.

Doctors may have expectations that are difficult to reconcile with compliance and security imperatives: in some cases, in order to move more quickly and process patient data more swiftly, healthcare professionals store or share medical imagery on free data sharing sites, easy to access on the Internet but without the necessary level of security. In one such instance in 2013, as was reported in the press at the time, a new mother was aghast to find, upon typing her own name into a search engine, data about her childbirth, openly available for viewing on the Internet. The CNIL responded by conducting with several verification missions on-site, in the wake of the article's publication.

“That's why”, Bruno Donius specifies, “the Privacy Officer is a stakeholder to the work conducted by a special committee, the CCIM (Medical Data Conformity Committee) in which doctors and para-medical professionals are involved. It is in charge, for instance, of setting the working rules for the care providers, and looking at the IT traces left when the hospital practitioner takes action in icebreaker mode”, he adds.

For all the above reasons, the CHRU's Privacy Officer has a special relationship with Management. “He reports directly to me”, says Bruno Donius, who expects his DPO to fulfil three key responsibilities: “gathering intelligence, keeping watch and raising questions when a problem arises”. A fourth responsibility, perhaps the most important, completes that list: raising awareness and educating. Guillaume Deraedt constantly works to explain to practitioners that, “IT in the hospital is not the same as in the home”. There can be no talk of putting confidential patient data on the Cloud, for instance.

Asked to sum up the experience over the past few years, Bruno Donius had very positive words about the work of the CNIL Registered Data Protection Officer: “We did not experience a single problem and the Privacy Officer has every reason to be in an establishment like ours”, he concludes.

AT ESSEC GROUPE, “THERE CAN BE NO LEAVING ROOM FOR CHANCE”

In the Grand Hall at CNIT La Défense, ESSEC Business School runs its continuing training programmes. ESSEC (Higher School of Economic and Commercial Sciences), founded in 1907, trains an international school body of managers about the economy of the future -- it also has a campus in Singapore.



“ I EXPECT MY
PRIVACY OFFICER TO
HAVE NO QUALMS
ABOUT SOUNDING
THE ALARM IF THE
SITUATION CALLS
FOR IT”

Jean-Michel BLANQUER
Managing Director,
ESSEC Group

Highly-connected, the School encourages the use of social networks and new information and communication technologies. ESSEC is the most influential European business school on Twitter. Data protection for students (4,800 in initial training and 47,000 graduates) is no buzzword for the school.

“We manage a tremendous amount of personal data”, explains Jean-Michel Blanquer, Managing Director at ESSEC Group, “It ranges from data on academic affairs to e-mails, statistics and any information regarding student affairs. Each student implies an entirely distinct pathway”. “Personal data protection is of fundamental importance to us, and the CNIL Registered Data Protection Officer unquestionably helps us in this aim”, he continues, “what’s more, when you have alumni such as Minister Fleur Pellerin or Cécile Duflot, you have to seal your information walls as tightly as possible”.

Patrick Blum was appointed Privacy Officer at ESSEC from as early as 2008. *“Functionally, he is part of the IT Department, but from the operational standpoint, he reports directly to me”, the Managing Director is quick to specify. “He can come to me at any point, without going through the hierarchical channels”. That direct connection with the person in charge of data processing, emphasised*

Mr Blanquer, is one of the factors guaranteeing the Privacy Officer’s effectiveness. If the hierarchical ladder is too steep to climb in a specific situation, thus impeding decision-making, the Privacy Officer’s impact could be lessened, *“I expect my Privacy Officer to have no qualms about sounding the alarm if the situation calls for it”, he explains.*

As one of the initiatives of which he is proudest since the appointment, Patrick Blum readily refers to employee awareness-raising, a very important focus for him. Consequently, he speaks each month at the *“integration days”* held to welcome new employees, share the key concepts in personal data protection and secure digital practices, and be identifiable by all as the key contact person on such issues.

In the opinion of Jean-Michel Blanquer, the DPO’s mission is very clear: *“I expect him to ensure that we are ‘shipshape’, if I may say so, on all aspects of personal data protection and compliance with the Data Protection Act. I also expect him to originate proposals and educate us in the everyday about the issues at stake. Last but not least, we want him to infuse all of our practices with the Data Protection culture, including the most innovative, and in particular, the new tools being adopted as part of ESSEC Group’s development”.*

The School’s Managing Director readily lists examples such as the future *“cognitive map”* which will enable students to track their personal strengths and weaknesses at each stage of their path forward. It is easier to understand, from that perspective, that personal data protection is more than a necessity for ESSEC - it is an imperative.

THE DATA PROTECTION OFFICER INSTITUTED BY THE EUROPEAN DIRECTIVE IS A TRUE TURNING POINT

Greater added value, a differentiating factor, optimisation, compliance, corporate social responsibility, transparency, trust, ethics... there are many reasons behind the decision to appoint a Data Protection Officer with the CNIL.



“ IT IS OF CRUCIAL IMPORTANCE TO APPOINT A PRIVACY OFFICER FROM AS EARLY AS TODAY TO BE READY TO MEET THE NEW REQUIREMENTS IN 2018 ”

Paul-Olivier GIBERT
Chairman, AFCDP

The European Regulation on Protection and Free Movement of Data was released in April 2016. The new rules, which are destined to replace those of our current Data Protection Act, will come into effect two years later, in mid-2018.

The stakes are high. The extremely sharp increase in penalty levels is, of course, one factor to take into account (the CNIL could, for instance, inflict monetary penalties up to €20 million or 4% of global sales revenue). However, no less important are the new expectations placed on companies today: good governance of personal data will, in upcoming years, be a central factor in the relationship between organisations and individuals. The new law on portability of data illustrates the European regulators' intention to re-establish a balance.

Organisations that appoint a Privacy Officer today will be able to start implementing the measures needed to be ready when the time comes. Contributing to the co-regulation, the DPO helps take apart the processes, re-open contracts with the sub-contractors, integrate new requirements into the tender processes without ado, and be in a position to notify - the CNIL, as well as the relevant parties, if necessary - of violations of data processing rules, wipe out data that should no longer be stored, and deliver to customers, prospects and all relevant parties the information owed to them, and review the level of securisation on immaterial assets.

It should be reiterated that the Data Protection Officer, a «Privacy Officer 2.0», is the real turning point offered by the European Regulation and will be expected to guarantee compliance with the European regulation in the organisation. The responsibilities involved are manifold and challenging: to carry out risk analysis and impact studies, to serve as the key contact persons in the event of personal data violations (ensuring that the said violation is documented) and as the contact point for the parties involved, ensuring that requests for access rights are satisfied within one month (as opposed to two, currently), etc.

Companies will need every bit of the two years ahead to prepare for this change in scale and rationale on personal data protection requirements.

AFCDP supports its members in this process, through initiatives as varied as focus groups, conferences, publications, interaction with the National Commission on IT and Freedoms, and its involvement in the Confederation of European Data Protection Organisations (CEDPO), which it co-founded along with its German, Dutch and Spanish counterparts to ensure that the professionals impacted could have a voice Brussels.

AFCDP was founded from as early as 2004, when the 95/46/CE Data Protection Act was ratified, officialising a new profession: “Correspondent in charge of personal data protection” (or Privacy Officer, CNIL Registered Data Protection Officer).

While AFCDP is the French Privacy Officer's representative association, it also encompasses a broader population. In addition to data protection professionals and DPOs appointed to the CNIL, it is open to any party with an interest in personal data protection. The association's wealth lies - amongst other things - in the wide variety of members it brings together. CNIL Registered Data Protection Officers, data protection officers, legal specialists and lawyers, human resources specialists, IT specialists, marketing and e-commerce professionals, CISO and security experts, quality officers, archives and records managers, professional ethics specialists, consultants, academics and university students.

AFCDP is both the place where professionals in private data protection can come discuss aspects of their practice in a laid-back setting, identifying and sharing best practices, as well as a forum contributing to the adoption of relevant and applicable rules by the legislative bodies, whether national, European or international.

AFCDP encourages discussion and information-sharing on personal data protection in order to facilitate communication between its members and promote best practices. AFCDP maintains dialogue with CNIL and other relevant authorities at the French and European levels impacted by personal data protection.

In 2011, working with the GDD (Germany), NGFG (Netherlands) and APEP (Spain), AFCDP established the European Confederation of Associations of Data Privacy Officers, CEDPO (www.cedpo.eu). Ireland, Poland and Estonia joined the confederation in 2014. The confederation gives a professionals impacted by the European Regulation on data protection a voice in Brussels.

Some AFCDP Members:

Accor - Action contre la Faim - Adecco - Aéroports de Paris - AG2R La Mondiale - Agence de la Biomédecine - Agence de l'Eau Adour Garonne - AGIRC ARRCO - AGPM - Airbus Group - Air France - Alcatel-Lucent France - ALLIANZ - Alstom - American Hospital of Paris - AMF (Autorité des Marchés Financiers) - Amiens Métropole - APCE (Agence pour la Création d'Entreprises) - Argosyn - ASIP Santé - Autorité de régulation des activités ferroviaires - Axa - Banque Neufilze OBC - Barreau de Lyon - Bayer Healthcare SAS - BioMérieux - BNP Paribas - BP France - Caisse d'Epargne Provence Alpes Corse - Caisse des Dépôts et consignations - CNIEG - Cap Gemini France - Carrefour - CCMSA - Cegedim - Centre Hospitalier d'Avignon, de Bordeaux, de Clermont-Ferrand, de Nice, de Poitiers, de Toulouse, de Bar Le Duc, de Bretagne Sud, d'Esquirol, de Mantes la Jolie, de Nemours, de Polynésie Française, Le Vinatier - CGOS - CCI de France, de la Région Alsace, de Grenoble, Marseille Provence, Rhône Alpes - Chambre Nationale des Huissiers de Justice - Cnaf - CNAMTS - CNP Assurances - CNRS - Coallia - Cofidis - Communauté de l'agglomération belfortaine, de l'Agglomération Saint-Loise, de communes de la Hague, Communauté Urbaine de Marseille Provence Métropole, Communauté Urbaine de Strasbourg, de Bordeaux - Compagnie de Saint Gobain - Conseil départemental des Alpes Maritimes, de Charente Maritime, de la Gironde, de Guyane, du Nord, des Pyrénées Atlantiques, de Seine Maritime, de Seine Saint Denis, du Val d'Oise - Continental Automotive France - Cour des Comptes européenne - CRAMIF - Crédit Agricole Consumer Finance - Crédit Coopératif - Crédit Immobilier de France - DHL Express - Digital & Ethics - Ecole Polytechnique - Edenred - EDF - EFS (Etablissement Français du Sang) - Electrolux - Engie - ESSEC Business School - FNAC - Foncia - Franprix Leader Price - Gendarmerie Nationale - Generali - GMF Assurances - Grands Moulins de Paris - Grand Port Maritime de Marseille - Gras Savoye - GRDF - Groupama - Groupe Auchan - Groupe Novalis Taitbout - Groupe Pasteur Mutualité - Groupe Prévoir - Groupe Randstad France - Groupe SEB - Groupement des Mousquetaires - Hachette Livre - Harmonie Mutualité - HENNER - GMC - Hospices Civils de Lyon - IBM France - IKEA France - INA - INED - INPES - Institut Curie - Institut Mines Télécom - Institut de Radioprotection et de Sécurité Nucléaire (IRSN) - Inter Mutuelles Assistance - Iveco - JCDecaux - Keolis - La Française des Jeux - Lagardère Active - La Poste - La Redoute - LDLC.com - Legrand - Lilly France - Lyonnaise des Eaux - MAAF Assurances - MACIF - MAIF - Mairie de Drancy, de Gennevilliers, de Montreuil, de Valenciennes, de Bordeaux, de Carros, de Lyon, de Marseille, de Metz, d'Oissel, de Paris, de Poitiers, de Villeneuve d'Ascq, de Vitry-sur-Seine - Malakoff Mederic - MAN Diesel & Turbo France - Manpower - Matmut - MBDA - Médecins du Monde - Michael Page - Michelin - Microsoft France - MMA - Mutuelle Nationale Territoriale - Naphtachimie - Natixis - Neotoa - NextRadioTV - Numericable - Olympique de Marseille - Orange - Orpea Clinea - Paris Habitat OPH - Philips France - Plastic Omnium Auto Exterieur Services - Port Autonome de Dunkerque - Priceminister - Promod - RATP - Region Haute Normandie, Ile de France, Midi Pyrénées, Lorraine - Renault France - Robert Bosch France - Sanofi-Aventis R&D - Scor - SNCF - Sodexo - Steelcase SA - Suez Environnement - Swiss Life - Technip - TNS SOFRES - Total - UbiFrance - Veolia Environnement - Vinci Energies - Xerox

www.afcdp.net

