SMEs – COMPLIANCE NOTES

Data Protection

Victoria Anzola, Seqqe

June, 2020

I train companies to be compliant with business laws, mainly in Data Protection and Anti-Money Laundering. I work both in Spain and Colombia. In Spain, the majority of my Clients are in the Málaga and Barcelona areas; in Colombia, in Bogotá and Medellin.

Table of Contents

Why these Notes? Majors vs. SMEs

I have compiled these notes so that I can share with others the experiences I have gained over the last 10 years. Most of the Data Protection colleagues I meet with at conferences are employed by large organisations, with in-house DPOs. The talk at these meetings tend to be heavily biased towards the impact of DP laws on major companies.

I work mainly with SMEs. I am conscious that these small companies represent over 80% of business employment in most countries. Furthermore, they often act as 'Processors' for the personal data of many much larger companies, whether as outsourced IT suppliers, or accountants, or lawyers. Even if the number of clients/suppliers/staff held by each SME is relatively small, in their totality the number is no doubt much higher than that held by the 20%-or-so major companies. I am conscious that SMEs do not get the attention their personal data volume should dictate. And a breach in personal data can be just as damaging to an individual whether the holding company is a major or a minor business.

On reading these notes, one might get the impression that I have highlighted only the worst cases I have come across. That is not so. The truth is, I have come to expect most if not all of the issues documented here with each new client I set out to train.

My Market in the Costa del Sol area, Spain

There are very few large employers in the Costa del Sol area, the vast majority (about 90%) having less than 10 employees and only a few (less than 3%) having more than 50 employees. This area is therefore totally dominated by SMEs (Small, Medium, Micro companies), with over 17,000 registered businesses. As in most cities of the Andalusian coast, the economy revolves around tourist activities. The service sector accounts for 60% of employment, while trade accounts for almost 20%. The main branches of the service sector are hospitality (hotels, restaurants), real estate and business services.

Cultural differences in Spain

A small but significant number of these companies in Spain are run by northern Europeans who migrated to the area for its fine weather and coastal Mediterranean lifestyle – UK, German, Scandinavian, Dutch, Russian... The majority were attracted firstly by the climate and Spanish life-style, but have had to make a living and therefore had to start their own companies – Cafés, real estate, medical services, financial services, builders, electricians, plumbers… Many are self-employed ("Autonomos").

These northern Europeans do not want any problems with the Spanish authorities. They tend to be more careful than the Spanish to ensure they are compliant with the Spanish business laws. On the other hand, anyone can come along and tell them what they need to do to be compliant. Their lack of inherent understanding of the Spanish and their ways can lead to schemes that end up taking their money without being provided with anything that makes them compliant. Often, this means a copy-and-paste version of the law bound in a folder and presented to them with the confident statement that "You are now compliant". Or they pay for a course in the particular law and on completion receive a Certificate, fully believing that this means they are now compliant.

I focus my attention on the northern European companies here in this area. In Colombia, many of the companies I train are local affiliates of international companies. Very often, and notwithstanding the competence of the HQ of such companies in the USA or Europe, the local employees are left to flounder in their limited understanding of the Colombian data protection laws.

Marketing Data Protection compliance training

Even with these, the 'sale' of compliance training can be difficult. It was easier when the Spanish DPA was fining companies for non-compliance with the data protection laws. But the recent prolonged period of non-government in Spain, coupled with the introduction of the European GDPR and the need of the Spanish Congress to incorporate the GDPR into its Spanish law has put a hold on inspections and fines, certainly at the SME level. One result is that companies have again buried their head in the sand, ostrich-like, assuming that if no one around them were being fined, then the law 'didn't matter'.

In Spain, a small percentage of a company's Social Security payments are intended to pay for in-company training. Much of the costs of training in compliance can be offset against this, making the effective training cost to the company retrievable. If it is not used in the year, the company loses that benefit. In these circumstances, one would think the sale of compliance training would be a no-brainer.

Not so.

The initial responses to an approach for compliance training in Data Protection in both Spain and Colombia usually go something like this:

- "I don't think we have to do this. We don't keep any personal data"
- "We only store data for other companies, so I'm told by our lawyer that we don't have to comply"
- "If we have to do it, let's do it quick – and don't involve me or my staff"

From the comments I have heard, I put this initial reticence down to the following:

- They don't understand what data protection means
- They think it's another senseless requirement by the government
- They don't see the monetary value in complying, except possibly to avoid fines – a gamble many are prepared to take.
- They don't want an outside body (i.e. me) investigating their business
- They don't want to pass information to governmental authorities because they fear being spotlighted for an inspection. (This last was more prevalent prior to the GDPR when companies were obliged to register their personal data files with the DPA in Spain. In Colombia, companies still have to register their files with the Data Protection Authority SIC into the RNBD).

- And they certainly object to paying one of their few staff members to do anything but that which they were originally employed to do. It increases their overheads.

Time taken to become compliant

Before I can estimate my training costs for a specific company, I need to know a certain amount of information about the company. For this purpose, I send them a Questionnaire which includes such non-contentious items as “Your company’s registered address“; “How many Departments do you have?”; “How many employees?”; “Are you a member of a Group of companies?”; and so on. From this information, I can prepare a quotation for my work, my price and time scale.

In my experience, a training programme that should take, at the most, 4 to 6 months, in reality will take a full year, and sometimes much longer.

Why?

Even with willing companies and a designated staff member (which I term “Compliance Representative” or “CR”) or (in a few cases with SMEs) a DPO, empowered by an initially-enthusiastic CEO, the amount of work involved is heavy.

Major companies may hardly notice the addition of an a DPO in their total manpower costs, even if at a high salary. Burdening an SME with a Compliance Representative in, say, a 10-employee company adds overheads that can break their profitability.

While the GDPR does not mandate that most SME’s need to produce a Data Protection Policy Manual, they **do** need to have their policies documented somewhere. The most useful format I have found is a DP Policy Manual, whether on paper and/or online in digital form.

I work with each company to train them to generate their own company-specific ‘bespoke’ DP Policy Manual. Each one is different in detail. This is a ‘living document’ which is intended to be continuously updated by the CR with information that records the aspects of the company’s data protection that change over time, such as password allocations, permission to transfer files out of the office, contracts with external Processors, and so on. The Manual is in 18 chapters, covering the whole gamut of the GDPR and any small modifications added by the Spanish law makers, and also covering the Colombian Data Protection law (which in many ways, closely duplicates the GDPR). All staff must be trained, for which I use my own online training platform (in both Spanish and English), as well as face-to-face training sessions with the company’s staff.

Other than the time taken up with this training, the CR will generally have another job, that which they were originally employed to do. Initially they feel burdened with this extra role. They are usually slow to complete the tasks I set them, such as deciding how they will gain the express consent of their clients, suppliers and staff. They take their time or lower the priority of the need to be compliant because:

- they have their other tasks; or
- they do not initially feel confident in dealing with a new subject; or
- they do not believe that the protection of personal data is important to their company.

Or they raise objections. When asking for an organigram of how personal data is moved between departments and for what purposes (e.g. from reception to marketing to invoicing to…), I've been told:

- "The information you are asking for is none of your business. "

or

- "It's impossible to know."

It can be an up-hill slog to overcome such reticence and to engender a state of trust with the CR.

And because the process gets prolonged, the original designated CR can leave, requiring a new CR to be designated by management. The initial difficult educating stages become a *déjà vu* performance.

Company organigrams and data flow

The service I provide is restricted to training. I have a training-focused processing contract with each of my client companies since I process their staff's personal data to set up the online courses. Part of the compliance training requires that the company runs an internal audit of where the personal data it holds is used by the various departments. Even small companies will have separate departments, even if each department only has one or two members (e.g. Sales, Invoicing….). Most companies I deal with have never looked at their business from the perspective of "who uses the personal data, and for what purpose?". The designated CR may not know all of the internal workings of the company they are working for, so it can become a voyage of discovery for the CR and for those they have to interact with to build the data flow diagram.

One of the few delights I receive from this work is when it begins to dawn on the CR and others in the company that they, through this data flow analysis, start to 'discover' how their company actually works and what the various departments do with the personal data they hold. This is usually when the CR's enthusiasm for the compliance task steps up a gear. Furthermore, this analysis can lead to a better understanding of how the company really works at a general level as an efficient or non-efficient organisation. Duplicated responsibilities and processes that are conducted differently by internal departments become exposed, usually leading to fundamental changes and standardisations in the company's processes. At this stage, these companies can start to see an economic value in implementing a compliance programme in terms of their overhead cost savings.

Late-entrant disclosures of additional companies

Sometimes I can be working with a company for several weeks when I come to organising the company's online training schedule. I now have a flow diagram of the various people in each department, names I need to enter into the online training platform. As has happened in a surprising number of cases, it is only now that I discover that some of the employees are 'missing'. On querying this omission, I discover that there is a second, so-far-undisclosed second company. Often the CR is not aware that some of their colleagues are hired by this second company.

Amongst other possible explanations for these initial omissions, I believe that it is often a result of how SMEs set themselves up, with changes over the years that are not realised by relatively new staff. I doubt that larger companies have similar internal issues, since they have the staff and professionals who keep track of such matters.

This realisation changes the wording of the various clauses in the data protection compliance statements. For example, which company is responsible for data security measures; which company are data holders providing consent to; and so on. In addition, it may be necessary to list two separate Controllers or Processors. All of this complicates the compliance progress and in many cases, causes the business to re-think and streamline its internal company structure.

Staff Confidentiality and Internal Rules

In order to meet both the GDPR and the Colombian requirements of employee non-disclosure and secrecy of personal data, I train companies to prepare Confidentiality Agreements for their staff to sign. In addition, I encourage the company to develop their own set of Internal Rules that govern how they treat the company's Data Security measures, again to be agreed and signed by staff. These go some way to mitigating the company's responsibility in the case of a data breach by, for example, a disgruntled ex-employee or an Autonomo who used to work for the company. In addition to the extra work required with the late disclosure of a second company, a second set of Confidentiality and Internal Rules agreements have to be created to be signed off by the relevant employees.

I have had occasions where individual employees have refused to sign such agreements, often because they have a distorted view of their own personal data rights and how such agreements will diminish those rights. It can take time to address and correct such misconceptions. In one case, the company was left with no option but to fire the objecting individual.

The need for Consent

My clients tend to have their personal data in totally unorganised and unstructured paper records and digital files. Many copies of an individual's data may be stored in

several places and used for different purposes, without one department knowing anything about another's usage.

One of my early tasks is to train the company on the need for Consent. Their first step is to consolidate their personal data information into a structured, single format that is the source for all departments and all usage (i.e. no duplicate files).

It sounds good on paper, but can be a cause time delays, additional cost, and internal friction (*'too many bosses, not enough workers'*).

The next question is "Do your files have the explicit consent of the data subjects for each of the purposes you are holding their data for?"

Companies fear that if they ask for consent, they may be told "No", and lose their Client base and with it, possible business.

There are also not infrequent cases where new sales staff bring a client list from their previous employment. As I make the company aware of the inappropriate nature of using others' data bases, they realise that they have to obtain the required consent. Some respond with the extreme step of erasing all external personal data (clients, suppliers). Some just quit the compliance process (too much work, no time and no money to pursue it).

Other will get organised and send out emails to their existing data subjects requesting the required consent. I work with the company to put together an interesting marketing approach to encourage the data subjects to provide their explicit consent, with the intent of overcoming the company's fear of rejection.

This seems to work some of the time, enabling the addition of value to one of the company´s largest assets, their client data base.

Security measures

Many small companies have not done anything about their data security. Very often these companies outsource their IT services. IT services for some companies are limited to picking up the phone and calling their IT contact to "Come and fix my computer. It's not responding".

In terms of data security, I observe that SME's fall into three categories, about evenly split:

- **Companies with 'nothing'**.
- **Outsourced IT services**.
- **In-house IT services**.

Companies with 'nothing': They have their website, often created by an IT specialist some years ago. They may no longer have the Admin codes to edit their website and bring it up to date with such items as a Privacy Policy or Cookies. IT maintenance of

their hardware and software is done on an *ad hoc* basis by bringing in an outside IT specialist. Some companies do their own backups, many don't.

Working with these companies is very slow, usually because no one in the company is particularly IT user-friendly. It means that they have to hire an IT person to do the work, over internal reticence and objection.

Outsourced IT services: Providing, for example, usernames and passwords, backups, server allocation, cloud software, but have never documented their work as part of a comprehensive security plan. These IT companies are often not even aware of the requirements of the GDPR or other data protection laws.

This can also be a lag on the journey to compliance. The IT service supplier may have little or no understanding of DP compliance. I am not paid to train these third-party companies and it takes time for the Controller to recognise that they need to pay the outsourced IT specialist to document their security measures.

It can take between 3 and 6 months just to get the documentation written by the IT supplier. I have encountered some IT specialists that have never been asked to document procedures before, have no idea of how to do it, and are ashamed of admitting it. This tends to be expressed by them raising objections to doing the job they are now being paid to do.

In-house IT services. This category applies to the larger SMEs, and includes smaller IT service companies (small SMEs do not justify an in-house IT specialist).

The larger the SME, the more likely they are to have documented some aspects of their data security. However, rarely does this completely satisfy the requirements of the data protection laws.

In my training, a compliance programme cannot advance unless security measures are documented and implemented.

Controllers, Processors and Lawyers' advice

In the cases where my clients are the Controller, they very often do not have any written agreement with their outsourced service suppliers (IT, Accounting, Legal, etc.…) i.e. Processors. I provide my clients with a model Controller-Processor contract that incorporates the required data protection clauses for those Processors who handle the personal data held by the Controller.

Some of these Processors have not even thought about the data protection laws. When they receive the Processor agreement from my client, they are shocked by the legal obligation such a contract imposes upon them. They will usually ask their lawyer to check the contract. This takes more time.

After 10 years of training companies in data protection, I should not be shocked by the frequency that lawyers provide their clients with the wrong advice. I had naively assumed that lawyers, when acting for a company, understood the compliance laws.

It would appear not. And a Processor, having paid for legal advice and been given the incorrect information, is a mountain to overcome. Other than discussing the specifics of the law with the Processor, I have often reverted to asking my client to find an alternate Processor that understands their obligations.

DPIAs and SMEs

The need for a DPIA for a typical SME is rare as hens' teeth. So far, I have not had to train any of my clients in how to conduct a DPIA.

Colombia - File Registration with the DPA

In general, these notes apply to both Spain and Colombia. However, one significant difference is the requirement for Colombian companies to register their files with the DPA. This used to apply in Spain, but post-GDPR, this requirement has been dropped.

The need to register files instils a discipline on companies to at least start the process of compliance. It is easy for the Colombian authorities to cross-check which companies have registered their files. In Spain, and in Europe, the law lacks this 'nudge' for companies to begin their compliance process.

ICO Registration fee

I note that the UK ICO is now charging every company a 'fee' to register with the ICO (albeit not for registering files). It would appear that by applying this annual fee, (not unlike road tax), every company will become aware or the data protection law. Given the overall poor record of compliance by SMEs across the EU (less than 50% in 2019), such steps may be necessary elsewhere to increase the awareness of the law.

Final Note - Covid-19 Lockdown and its impact on training

Before the Covid-19 pandemic forced us to change the way I interacted with my clients, I would regularly visit the companies in their offices. That has changed – and for the better. I am now dealing with by clients online, developing the various documents for their DP Manual with them. These online meetings are much more focused, less 'sociable', less likely to be interrupted and much more productive. In addition, I don't have to spend the time and money driving to and from their offices, a more cost-effective and greener option for me. My clients confirm that the online process is better for them. We agree the work load to be carried out by the Client Representative before the next scheduled meeting, that typically takes about 30 minutes to 1 hour.

Victoria Anzola and Short Allerton. Seqqe Group