TenInsight

TenIntelligence

www.tenintel.com | May 2018 | Issue 3

# Our GDPR Journey so far

Not everyone will be ready or compliant by 25th May, but the Information Commissioner's Office (ICO) will require you to demonstrate you have made a concerted effort to start. We learnt a lot during our own internal GDPR preparations and I would like to share some of our experiences with you.

We started our journey in February 2017 when we embarked on the ISO 27001 process for Information Security Management. We wanted to demonstrate to our clients that we take security seriously, especially when we are handling sensitive information.

As you can imagine, as part of our due diligence and employment screening services, we handle personal data on a regular basis in the form of items such as CVs, passports, application forms and university certificates.

As part of our ISO accreditation, many processes and procedures we were putting in place also met with the requirements under requirements for protecting personal data according to GDPR.

From our experience, communicating the importance of data protection from senior management to the rest of the team was pivotal. Everyone understood quite quickly why data protection is vital to the success and reputation of our business.

Our team recognised what the impact GDPR will likely have on our operations. Conveying this message across early and reinforcing our internal culture regarding data security was our first step to compliance.

**Neil Miller**

CEO, Ten Intelligence Limited

*See page 2 for full details of our journey.*

# ISO27001 recognition for TenIntelligence

TenIntelligence is pleased to announce it has been awarded ISO 27001 certification and successfully implemented an Information Security Management System (ISMS).

Following an extensive audit carried out by the British Assessment Bureau (an UKAS accreditation body), the firm received its official certificate of registration in March 2018.

Neil Miller, Chief Executive Officer, said: "Confidentiality, integrity and the protection of data are paramount to our clients – and our latest accreditation ensures we operate with best practice. It was a real team effort and I thank all of our staff for making this possible.

"Having ISO 27001 in place minimises the risk of potential data security breaches and reduces errors and costs, while demonstrating credibility and trust."

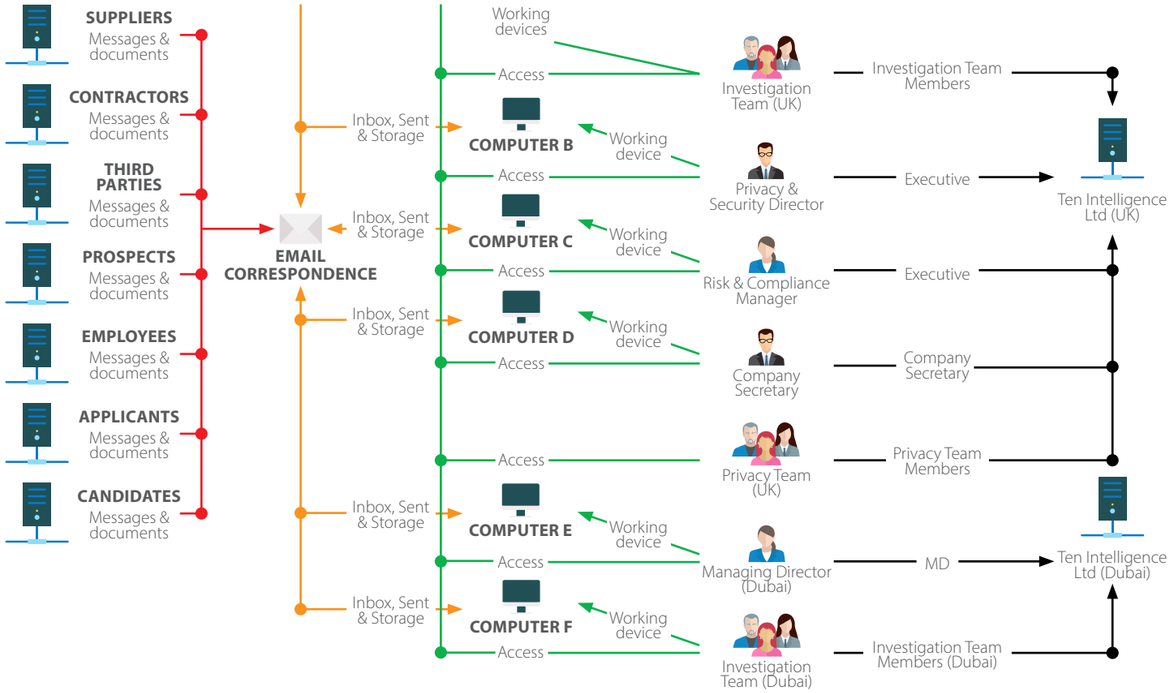
Richard Bell, Privacy & Security Director at TenIntelligence, added: "We assist clients with their readiness and continued compliance for GDPR, Cyber-Security, Data Breach Investigations and Incident Response. It was extremely important we demonstrated to our clients and contacts that we take data protection seriously and our internal procedures and culture are recognised to an international standard."

The company was assessed across several fields including relevant documentation, the scope of its ISMS, Business Continuity, Risk Assessments and internal procedures as well as control checks appropriate to its business and services.

## Acquisition International magazine has awarded TenIntelligence Best for Hedge Fund Due Diligence and Background Checks at the recent 2018 Hedge Fund Awards.

The awards are judged solely on merit and are given to those most deserving for their ingenuity and hard work.

Chief Executive Officer Neil Miller welcomed the prestigious award: "We are delighted that the Hedge Fund industry has again recognised TenIntelligence as an outstanding performer in the due diligence arena. We continue to protect our clients from investment risk and regulatory breaches through analytical insight, due diligence and risk compliance. This award is down to the exceptional effort that our investigative teams in the UK and Dubai provide our clients."




## Mapping your data

Until you address GDPR, you'll never be compliant or even working towards compliance. Take some time out with no distractions and list where you think data is stored.

This will help form part of your data mapping. Keep it simple to start with, consider:

- How do you obtain personal information (from the data subject, email, post, website, CCTV etc)
- What information is collected (name/ date of birth, passport, utility bills and banking details etc)
- Where do you store the data (PCs, tablets, printers, mobile devices, cloud-based technology)
- Who has access and whether any third parties have access to the data?
- Do you share or transfer personal information with others outside the EU, and if so, where?

There are several ways of mapping this phase. We used a product called i2 Analyst Notebook to help map our data or "information flow"; but you can use a simple flowchart within Word, or even a large flipchart or board. This will bring your data mapping to life and you will be able to see and add to your map as the process continues.

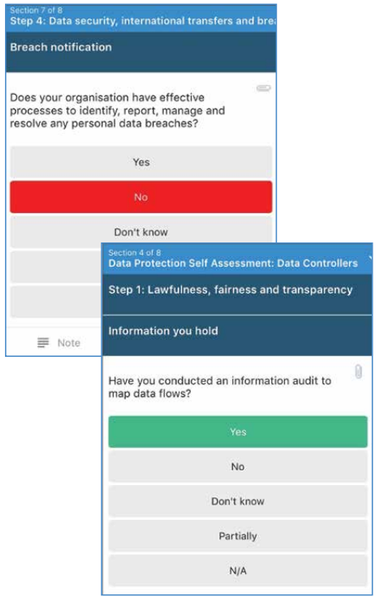
## Questioning

As part of our audit process, we examined where our internal personal data was held, how we processed it and whether it was secure. We then drafted an internal document that questioned our internal procedures.

We considered our procedures from a human resources and operations point of view. From the recruitment process to those that leave; who has access to payroll, personnel folders and cloud platforms (where are our cloud platforms?); how do we send and receive information to and from clients? Do we process any personal information on children?

Do you know whether your data subjects are notified of the collection and processing of their data? Do they know why their data is collected and who it is shared with? Is this communication easily accessible, concise and transparent?

What about email? What procedures are in place for receiving and sending personal information via email? Is personal data only used and stored for the purposes it was originally collected for?




These were just some of our starting questions.

Once all the responses are collected, collate the answers into one report. This will identify the areas of good practice, development areas and points for concern. This process forms part of your gap analysis, which you can revert to, once items of concern have been addressed.

**If you're interested, we can share our pre-assessment questionnaire tool with you.**

Once the internal data mapping process was collated, we then applied the same questions and processes to our clients' data.

We then added the findings and data flows onto our data map. I would really encourage this.

## Legal Terms

At some point in the GDPR preparation, you will likely need legal advice as to what your contracts and privacy notices will need to cover.

Your contractual obligations will differ depending on what services your organisation provides. You will need to determine the legal bases and legitimate interests you implement to control or process the personal data of EU citizens.

Some legal points to consider include:

- employment contracts
- current consents
- privacy notices
- opt-in or opt-out
- terms of business
- third-party written agreements
- engagement letters with your clients
- website legal notices, etc.

Again, your data mapping will help point your legal advisors towards the areas where you will need assistance.

Having identified your data, analysed the gaps, mapped your processes and spoken to your legal advisors, you have achieved most of the hard work.

## Internal process changes

You will also need to update your internal policies and procedures to reflect the changes to your GDPR readiness and communicate these to your employees and third parties. Don't assume that everyone will comply with your request, talk with them too. Make it part of your organisation's plan to implement regular Data Protection and Privacy Impact Assessments.

Decisions like how long to retain personal information should be set; who has access to the information (and who does not need access); keeping a record/ register of the consents you have; and reviewing your ongoing relationships with individuals and their data.

Consider also the procedures you will follow if you ever have the misfortune to detect or report a breach. Does your organisation require a dedicated Data Protection Officer (DPO) or someone to take responsibility for data protection compliance? Who and where do you report a breach to? Do you outsource your data protection compliance?

## Register with the ICO

Finally, which many organisations forget to do, register your organisation with the Information Commissioner's Office or if you are based outside the United Kingdom, a relevant supervisory authority.

GDPR will be organic and change over time. Over the next couple of years, precedents and further guidance will become available, whilst success stories and failures will be reported. Keep monitoring the developments, continue to audit your processes and keep your internal housekeeping in order.

If you make data protection part of your working day and culture, it will soon become much more manageable.

However, if you haven't done so already, make a start.

**For GDPR assistance, please contact Richard Bell or Sonel Martin by calling +44 (0)20 3102 7720 or email info@tenintel.com**

# Ransomware First Aid & GDPR

In plain terms, ransomware is a type of malicious software that locks users out of their IT system until they pay ransom to the attackers.

The attackers usually gain access through email or social media, luring users into clicking on infected links, which quickly spread malicious code that encrypts the system files, making them unreadable and inaccessible.

A message is then displayed, demanding ransom. The premise is clear: if the user doesn't pay, they lose their data permanently. A time-limit is usually imposed, after which, the price will increase significantly.

Ransomware is a profitable activity for cyber criminals. However, even if payment is made, there is no guarantee the files will be recovered and that data will not be made public. Business should, therefore, take cybersecurity seriously, even more so with the introduction of the GDPR.

Once a business has fallen victim to a ransomware attack, there is no easy way to recover. Reputation harm, loss of clients and public criticism add up to financial losses and threat of lawsuits. This is why some businesses may decide to keep quiet. However, the added damage to your reputation once it becomes known you have tried to cover up any data breach will be hard to repair.

Self-reporting is advisable, and with GDPR coming in force, it will be mandatory. Data Processors and Data Controllers will have 72 hours to notify the ICO from the moment of discovering a breach.

Once a breach has been notified, the ICO is likely to launch an investigation, looking particularly at whether you had appropriate measures in place to protect the data you held.

Article 25 of the GDPR specifies that technical and organisational measures shall be implemented by Data Controllers and Data Processors for data compliance, proportionate to the risks of the potential loss of data. Examples of the types of measures to put in place include:

- Ensure data is processed only on instruction and persons generally having access to the system have either controlled or no access to sensitive and personal data.
- Train everyone on the network to an adequate level. Giving admin rights to untrained personnel poses a huge risk, as admins can change files on the system, and if the system falls victim to cyber-criminals, they have the power to exercise full control over it. Two-factor authentication system may strengthen log-in attempts.
- Deleting files and emptying the recycle bin is not enough, as even deleted files can be recovered by the attackers. It is advisable that businesses subscribe to data-shredding software.
- Antivirus and anti-malware software must be up-to-date, suitable for the needs of the business and offer real-time protection.
- When necessary to click on a link, the use of content filtering may be handy. Content filters check the link against malicious site databases and ensure the visited page has up-to-date security protocols.

*Continued on page 4*

- As noted, infection usually happens via infected links and files. Users must be extra vigilant when opening an attachment and always check for a hidden file extension. (For example, a text-file is not supposed to have an executable extension ".exe").
- Disable protocols that are not in use.
- Use strong passwords, which are a mix of capital and small letters, digits and symbols. It is not advisable to use the same password for everything. Furthermore, passwords must be changed regularly and never shared.
- Backing up is vital for restoring files quickly. The back-up folders must be inaccessible, ideally on an encrypted portable hard-drive that is kept disconnected from the network. When backing up the files, it is advisable to do so offline.
- Data-encryption means that even if control over the system is seized following a ransomware attack, the files will be of no use to the attackers as they won't have the decryption key.

If an infection occurs, adequate decision-making will be vital. At this point, crisis management and business continuity plans will be invaluable. In the first moments of a suspected infection, disconnecting the machine from the network or its forced shutting-down may play a crucial role in attack prevention.

While it may sound complicated to those who have no IT background, it is important to remember that the best defence against ransomware is prevention. If you need any help with becoming GDPR-compliant our Privacy Division can help. Please let us know or visit http://www.tenintel.com/audit-assessment/

For Sanya's full article please visit www.tenintel.com/insight

# Updates from our Dubai office

## High End Luxury Jewellery Factory – Instagram - Dubai

One of the largest law firms in the Middle East instructed TenIntelligence to carry out investigations into an Instagram account which was marketing the sale of counterfeit luxury jewellery. The case lasted over three months owing to the fact the account holder was not a UAE resident.

TenIntelligence operatives together with the assistance of local law enforcement were able to identify the location of the factory where the high end jewellery was being manufactured. A raid on the premises secured over 10,000 pieces of precious stones, gems and other jewellery shaped in the form of the client's trademark.

## Approximately 30,000 pieces of counterfeit items seized from a farm in Sharjah

TenIntelligence conducted the largest raid to date at a farm located in Sharjah, UAE. The estimated seizure was worth approximately 500,000USD, with the products occupying three truckloads. The goods are now secured in a storage facility and will remain there until the issuance of their destruction from the Courts.

## TenIntelligence invited to attend the Dubai Customs workshop ahead of IPR week

TenIntelligence received a personal invitation to attend a workshop hosted by Dubai Customs ahead of IPR Week. The IPR Workshop is a week-long event held by Dubai Customs each year to mark World Intellectual Property Day (26 April). The event was attended by customs inspectors and officials, together with other UAE government departments and private sector vendors and brand owners.

## Marcura appoints TenIntelligence for GDPR Support

The Marcura Group, a Dubai-based group of companies focused on providing innovative business solutions to the maritime industry, has appointed TenIntelligence's Richard Bell as its external Data Protection Officer (DPO). This appointment follows the recent hiring of Peter Meyer as a Data Protection Specialist working under the Group's Legal & Compliance Department.

These appointments strengthen Marcura's ability to comply with GDPR and similar international data protection regulations.

Richard Bell will serve as an independent consultant for the entire group. He heads up the TenIntelligence Security & Privacy practice, advising companies in Europe, Middle East and United States on physical and cyber security matters. Richard has extensive experience in this area and regularly works with the National Cyber Security Centre (NCSC), National Crime Agency (NCA) and the Information Commissioner's Office (ICO). He is a Fellow of The Security Institute and a Member of the Association of Security Consultants.

Peter Meyer works in close coordination with Marcura's Information Security Team in order to improve the governance of information handled and processed by the Group.

**Due Diligence | Investigations | Brand Protection | Privacy**

**Contact Us**

**UK**
+44 (0)20 3102 7720
info@tenintel.com

**MIDDLE EAST**
+971 (0) 4333 4669
dubai@tenintel.com

@tenintelligence