satswana

Company registered number 09329065 www.satswana.com

Consolidation document of advice to Councils to end 2019

Some of the advice to be found here will now be out of date, but still perhaps interesting in a historical perspective; other information will remain current, and hopefully useful. Please review the following contents to find any articles you need.

CONTENTS

satswana

Company registered number 09329065 www.satswana.com

A Council GDPR update, end 2018

At the end of a momentous year for compliance this update is intended to inform our Council customers, both with specific information and also referencing the documentation available to assist you under the ”Resources” tab on our website, www.satswana.com

1 Congratulations

First we must say well done to all of you, because in a recent survey when respondents were asked how far along they were in achieving GDPR compliance, only 29% said they had implemented all necessary changes. You remain amongst the leaders.

Secondly, to advise that Charlotte (“Charlie”) Smith, who is our Manager with special responsibility for Councils is due to produce her second baby in mid-January, and yet has been cheerfully trying to book meetings on the planned day! The team will not allow her to do that, and we will rally round for the first few months, needless to say, but she is still keen to hear from you and can answer questions on email and by phone!

2 Breaches

We have had a few – none serious, but the City of York's hack of a council app that affected 6000 residents was perhaps an object example of how not to handle things. Correctly they deleted the app, removed it from app stores and advised users to delete it from their devices. They were alerted to it by a developer from a technology company who had contacted the Council in line with its own guidelines. They thanked the person by reporting him to the Police!

He had not exploited the vulnerability, merely discovered it and reported it. His employer commented "There is an established precedent in the UK for legitimate security researchers to disclose vulnerabilities within information systems to relevant security teams. The Council's positioning of this good-faith disclosure as a deliberate attack flies in the face of the UK Government's National Cyber Security Centre advice on the matter, and the International Standard framework for vulnerability disclosure."

Fortunately the Police showed more common sense saying "they did not regard the incident as criminal. We recognise the benefits of software vulnerability disclosure as part of a healthy security environment and the researcher has acted correctly. There are times when 'researchers' overstep the mark but this is not one of those. We'd rather work with public-spirited individuals and share learning than criminalise people who act in good faith."

York's very weak response sought to partially justify their action "Whilst we consider we took appropriate measures based upon the facts at the time, we can now confirm that this was a well-intended action by the individual concerned and we would like to thank them for raising this matter." How many points would you give them for that?

Please note that if you think that you may have suffered a breach, of any sort, that we as your DPO should be the first line response. We now have considerable experience of handling all sorts of situations, and very often can use the "no risk to persons" ICO guidance to manage it internally. In any event, it is our job to formulate the reporting to the ICO, so please make us work!

3 Resources

In the introduction we mentioned our Resources tab, and you will find a great deal of information there, much of it with a Schools bias, but all the technical and regulatory aspects will apply equally to Local Authorities. If we can explain, we now have hundreds of schools we look after, many with around 200 staff, some with 500 and others (within Trusts) in the thousands. We continuously learn from exposure to the very capable resources within these schools, and seek to share that knowledge amongst all our customers. We hope you can adapt the advice to your own needs.

We will mention the Guidance Manual under the next heading, but the update notices published normally have specific advice that you may wish to browse – and issues such as our views on the EU/US Privacy Shield are likely to be of general interest. The commentary on the NIS directive is applicable to any organisation with a network, and the "Implementation Principles" can be used as a guide by anybody – you may well wish to review your status against these headings.

This document will also be added to the list!

4 Processor Agreements

If you share data with a Processor, where you are the Controller of the data, then you must have an appropriate agreement with them. We go into that at great length within Appendices D, E and F in the guidance manual under Resources. (The rest of the manual does have a schools bias, but also has general interest and relevance. We increasingly seek to publish this as a "knowledge base", so once again; please review it for any relevance to your situation.)

We will not repeat the content here, save to say that it remains one of the most difficult subjects to resolve, and one that is likely to still take you some time – do please read Appendix D to obtain the full argument!

If you have an issue with a Processor, ask us to help. The other day, after four iterations, we finally got a supplier of Allotments Software to produce an acceptable format. They had started with a compliant document under the 1998 Act, but were busy people and tried to bluster their way to getting the City Council involved to accept something that was not good enough, stating "much bigger Councils have accepted our contract". Satswana were certainly regarded as "the wicked witch in the west" until the supplier finally sat down and adapted our Appendix F to their

purpose, by which time everybody was happy, and we hope that their sales go well from now on!

5 Subject Access Requests (and FOI)

Please read our paper on Dealing with Subject Access Requests (under "Resources"), as this covers the specific precedent established with ICO in the University of Worcester case. Essentially it supports a degree of "executive privilege" in responses that may be particularly useful to Local Authorities.

6 Data Protection Fee

Regulators fund themselves from the fees they charge, so you can bet that they are keen to collect them, and they have started fining non payers (though fines go to the Treasury!)

Organisations that have a current registration (or notification) under the 1998 Act – prior to 25 May 2018 – do not have to pay the new fee until that registration has expired. You can check if your fee is due for renewal at https://ico.org.uk/about-the-ico/what-we-do/register-of-fee-payers/

7 No fear!

Of course we are specifically against the "fear" approach to compliance and Information Commissioner Elizabeth Denham insists that the ICO's response measures aren't punishments. "The law is designed to push companies and public bodies to step up their ability to detect and deter breaches," she said. "What is foremost in regulators' minds is not to punish the organisations, but to make them better equipped to deal with security vulnerabilities."

She added: "We understand that there will [still] be attempts to breach organisations' systems, and that data breach reporting will not miraculously halt criminal activity. But the law will raise the level of security and privacy protections across the board."

Important therefore to remember that the reason we are doing all this is because we are permanently under attack and if a criminal can get hold of the data we hold, then they can exploit it for monetary gain. It remains a dangerous landscape, and we have to be constantly on guard.

Happy Holidays, more in 2019. We are always delighted to hear from you with any queries, issues, or indeed experience that we can share. If a group of you get together for a meeting (or you have Councillors to bring up to speed), and you want one of us to attend to update as a briefing then please let us know. Attendees do not have to be customers, but we will seek to recruit them!

B Spring Council Update from Satswana

If you are a regular reader of our Resources content then you may have read some of these articles before, but they have been reproduced in a single document specifically for our Council customers.

Contents

Let's start with a pat on the back for our customers since in a recent survey, when asked how far along they were in achieving GDPR compliance, only 29% said they had implemented all necessary changes. Thus you are all "thought leaders" in this field.

1 After Brexit?

Hard or soft, little will change if you process data only in the UK, but you will still have to apply GDPR to anybody whether they are a customer, pupil, or parishioner who is European within your database.

The Government stated: "The EU (Withdrawal) Act 2018 (EUWA) retains the GDPR in UK law. The fundamental principles, obligations and rights that organisations and data subjects have become familiar with will stay the same. To ensure the UK data protection framework continues to operate effectively when the UK is no longer an EU Member State the Government will make appropriate changes to the GDPR and the Data Protection Act 2018 using regulation-making powers under the EUWA."

The Government plans to issue more detailed guidance in the next few weeks, but have said that the new regulations and detailed guidance will:

- Preserve the GDPR in local law;
- Confirm that the UK will transitionally recognise all EEA countries (including EU Member States) and Gibraltar as 'adequate' to allow data flows from the UK to Europe to continue;
- Preserve the effect of existing EU adequacy decisions, including the EU-US Privacy Shield, on a transitional basis;
- Preserve EU standard contractual clauses and binding corporate rules authorised before Exit Day;
- Maintain the extraterritorial scope of the UK data protection framework; and
- Require non-UK controllers that are subject to the UK data protection framework to appoint a representative in the UK if they are processing UK data on a large scale.

"On Exit, the ICO will not be a supervisory authority for the purposes of the EU GDPR and so will not be an EDPB member."

2 PECR

An amendment by the Government to the Privacy and Electronic Communications Regulations that increased the maximum penalty for violations to half a million Pounds took effect on the 17th December 2018.

Whilst not GDPR, PECR is closely aligned and controls marketing communications - and now there is particular danger for Directors as the ICO (Information Commissioner's Office) has the power to find them personally accountable for violations. This applies even if their organisation goes into liquidation or they are no longer in a senior position at the company. This rule is intended to make it harder for those who breach the law to set up a new organisation and carry out similar non-compliant activities.

3 No Fear!

However, let us repeat the mantra that a properly structured organisation has nothing to fear; indeed the Information Commissioner Elizabeth Denham insists that the ICO's response measures are not geared to punishments. "The law is designed to push companies and public bodies to step up their ability to detect and deter breaches," she said. "What is foremost in regulators' minds is not to punish the organisations, but to make them better equipped to deal with security vulnerabilities."

"We understand that there will be attempts to breach organisations' systems, and that data breach reporting will not miraculously halt criminal activity. But the law will raise the level of security and privacy protections across the board."

4 All websites should be HTTPS

Apparently 20.9% of the top 100,000 websites still do not use web encryption at all. Please make sure you are not amongst them! If you are HTTP you will find that many browsers will now flag your website as being "insecure".

5 Data Care Act?

Do not hold your breath, but there is a movement within the US to pass an act of this name that will get closer to the principles of GDPR. However, we do not expect this particular Leopard to change its spots on data privacy any time soon.

6 New risk identified for Mac's - MAC.OSX.AMCleaner

Apparently this 'scareware' is primarily delivered by email to trick victims into installing fake cleaning software, and the report notes that "anyone who thinks Macs are invulnerable to malware are sadly deluded".

In one variation, the malware opens an HTML page that is stored in its contents. In another, it is a full application that shows false scan results. In both instances, the malware prompts victims to purchase a fake malware cleaning service.

Anyone who follows the link to buy the cleaner is taken to a malicious domain and prompted to download and install the bogus cleaning software. When the malicious installer is run, it is actually signed with a valid Apple-issued certificate. This valid certificate allows the malware to bypass macOS protections such as Gatekeeper, and helps trick the victim into thinking it is safe to run the software.

7 Prize for the worst PR following a breach?

This prize has to go to Ticketmaster who blamed a supplier (Inbenta), who then responded "Upon further investigation by both parties, it has been confirmed that the source of the data breach was a single piece of JavaScript code... Ticketmaster directly applied the script to its payments page, without notifying our team. Had we known that the customised script was being used this way, we would have advised against it."

A caution for us all there however, as it is routine for programs to seek to access data from other sources. We must check in future that there is no possibility of exfiltration, since if we just accept the code as Ticketmaster did, then it is you who will take the reputational hit.

8 Extortionists Lie!

Now there is a surprise. GlobeImposter ransomware victims have found themselves abandoned by their extortionists, so if you did not have a backup, you are well and truly in trouble. Those who were encrypted and tried to pay found that the recovery procedure did not work. Because backups can also be infected, Satswana advises that you take a monthly "Archive" copy of your data. If all is lost, you may have to recreate several days information, but at least you have most of your history.

9 Just how dangerous is data?

To prepare these reports Satswana spends considerable time reading up on every possible source, and we copied this without noting the writer, so with apologies to them for not acknowledging their copyright, it is nevertheless very thought provoking.

"Until now, cybercrime was all about making money and stealing information (because information is money). Today however, we have the ability- from 30 feet

away- to shut off someone's pacemaker. A malicious individual could walk down a street today, and shut-off bodily devices that are controlled by computer chips, murdering them. In a few years' time, they will be able to do this from thousands of miles away. A law enforcement agent today can stop a vehicle on the freeway providing they are within 35 feet of it, because the average vehicle has over 240 microprocessor-controlled components; you can shut it off, lock the doors, enable airbags…. In a few years' time, a malevolent individual may be able to do that from thousands of miles away, on mass. Today, we think of cybercrime as financial crime, but I fear it will become much darker, more of a terrorist tool, and much more harmful to our wellbeing."

10 Prosecutions do take place

Notwithstanding our "no fear" message in item 3 above, the ICO have prosecuted and fined a former deputy head teacher for unlawfully obtaining personal data from two schools he had previously worked at.

This is also relevant to Local Authorities, this week we have had an incident of a Councillor obtaining and retaining information improperly. They must be clear that this exposes them to prosecution

In the School's case Darren Harrison was suspended from Isleworth Town Primary School only six months into his new role, having uploaded large volumes of sensitive personal data from Spelthorne Primary and The Russell School in Richmond to Isleworth Town Primary's server via a USB stick.

He was unable to provide a valid explanation for how the information had appeared on the server, and claimed it had been deleted. He later told the ICO that the data had been taken for professional reasons. Because he had no lawful reason to process the personal data, he was in breach of data protection legislation and was fined £700 under the Data Protection Act 1998 and ordered to pay £364.08 costs and a victim surcharge of £35.

Mike Shaw, the ICO's criminal investigation group manager, said: "The ICO will continue to take action against those who we find have abused their position of trust."

11 Critical Data

Have you got a securely archived note of all the critical user names and passwords that trusted staff use to access sites and information that are essential to your operation? It may be HMRC, VAT returns, bank access details, or even something like a Twitter account. The "knowledge" may be within the head of one person, as it was in the case of a Bitcoin exchange in New York. When the Founder died at the age of 30 millions of Dollars' worth of customer's assets became irretrievable because nobody else knew the access codes.

Of course, how you resolve having the information recoverable and yet keeping it secure is going to be an individual challenge but if it is essential to the organisation, you must find a way.

12 Digital Security Certificates

A research organisation has advised that there has been a wave of large scale DNS (Domain Name Server, the device that turns an IP address into a name you can read like something.com) hijacking attacks affecting dozens of domains belonging to government, telecommunications and internet infrastructure entities across the Middle East and North Africa, Europe and North America, since 2017.

Since the origin was alleged to be Iran, it was even more embarrassing for the US that certificates could not be renewed during the recent shut down of their administration! Without the HTTPS security miscreants can intercept and redirect web traffic, and you do not want that happening to your tax return!

Make sure your web certificate is up to date.

C September Update for Councils

Contents

1 Technology

We are delighted to receive news of considerable achievements within the Council community in the adoption of new technology, and must credit you for embracing change, using GDPR as a focus to improve procedures. That has to be the reason that we have so little to report by way of data threats or penetration, a credit to everybody.

One "qualification" that you might decide to advertise as a consequence is "Cyber Essentials"; you can find the details of this Government scheme here https://www.gov.uk/government/publications/cyber-essentials-scheme-overview

It has two interesting aspects, the first being the discipline that it brings to any organisation that goes through the approval process. When Satswana did it we found we learned a considerable amount and (despite our cyber background) identified many areas where we could improve our protection.

The second is that the original concept was that the Government would only engage digitally with organisations that met the standard. Now that seems to us to be a worthy idea. Do you really want to share any sort of data with a supplier who has not been as careful as you have been to protect that information?

There are a number of organisations that can provide support, and indeed you can "do it yourself", but Satswana found training value in being supported by expert help in order to pass the exam! The Business Manager at the Trident Group has been proactive in broadcasting the benefits, and he can be contacted at aaron.mouland@tridentgroup.co.uk

2 Data Retention

The Information and Records Management Society have updated their data retention guidance for 2019 and further details can be found on their website here https://irms.org.uk/. The criteria can be very confusing, especially when referring to governance and legal issues, some of which may be permanently archived. However a basic fall back rule, exactly as the legal basis for financial data, is current year plus six years.

3 Ransomware

To note that US local Councils have come under attack over the last six months. May we stress again our suggestion that you take an "archive" copy from time to time that (however out of date) would give you some history to go back to if you are attacked? The problem with ransomware is that the attacker only needs to deny you access to information that is critical to you. If your only option turns out to be to pay for release, then if they find a rich seam of people doing exactly that (as has happened in the United States) they will of course concentrate their attack on a soft target. Beware

though, that they may not play by Queensberry rules, there are many examples of people paying a fee, but then not being released!

4 Brexit

With apologies for using that word, but we covered a possible risk to data access in Item 1 of our February update here
https://www.satswana.com/resource/SatswanaFebruaryUpdate.pdf

That was pending March, with October pending now perhaps it is worth a read again?

5 SAR consent

In an interesting exercise a guy (with his fiancées consent) sent out a Subject Access Request asking for the information held on her. 40% responded without question. The good news really is that 60% did not, but we should all be aware that only the actual person concerned can give consent, and you must receive that directly. We suggest that is very applicable to the manner in which the Police are currently automatically generating requests whenever anybody is involved in a case, regardless of its relevance (paranoia that there "might be something"). It often contains an "authorisation" from the person, but we say you cannot accept that from a third party, even the Police. Our experience is that a refusal to supply unless a very specific aspect of data can be defined is normally not followed up.

6 European Representative

We will avoid using the word in 4 above again, but there may be circumstances where elements of your data holding will require you to have a continuing representative in Europe, in which case Satswana can provide that at no extra charge. (In the town of Aubusson for students of Tapestry!)

7 Subject Access Requests

It may be of interest to Councils that, noting the Ofsted commentary regarding rogue parents making life a misery with emails, Satswana (in conjunction with a number of other DPO providers) sent a submission to the ICO stating that SAR's were similarly unacceptable "weapons" in the hands of a certain category of bully or opportunist.

Our experience of FOI's or SAR's to Councils is that it is a similar sort of "character" who chooses to attack public officials and volunteers in a similar manner.

We interpreted the ICO response as being very sympathetic, but they are law enforcers, not law changers. Having said that we have found increasing ways of using exemptions and other techniques to lessen the burden (and sometimes significant stress) on staff, often through determinations provided by the ICO to the classic "I know my rights" merchants who submit a complaint.

Fact is that they actually do not know the state of current case law and precedent, and as a consequence their complaint has always failed. Thus if you get one, please call us in, that is what we are here for.

D Final Council Update 2019

"We are in an age of borderless data flows. And as data travels internationally, so do privacy issues. Microtargeting. Surveillance. Our digital footprint and the transparency expectations that go with that. Governance around data protection and meaningful privacy enforcement are more complex, multinational and political than ever."

Elizabeth Denham, Information Commissioner

Contents

1 CCTV installations

Following a request from a Town Council we have now done the research to ensure that we know what agreements are required for a CCTV installation, so if you have a requirement, please ask us!

Arising from that we noted an interesting amendment to the Freedom of Information Act following DPA 2018

If a request for images is received via a FOIA application and the person requesting is the subject, these will be exempt from the FOIA and will be dealt with under the Data Protection Act 2018 and GDPR.

Any other requests not involving identification of individuals can be disclosed but only if it does not breach the Data Protection Act 2018 and GDPR.

2 Special category data

The ICO has published updated GDPR guidance regarding special category data.
The GDPR singles out some types of personal data as likely to be more sensitive, and gives them extra protection. Special category data relates to personal data that:

- reveals **racial or ethnic origin**;
- reveals **political opinions**;
- reveals **religious or philosophical beliefs**;
- reveals **trade union membership**;

- **genetic data**;
- **biometric data** (where used for identification purposes);
- data concerning an individual's **health**;
- data concerning a person's **sex life**; or
- their **sexual orientation**.

3 Overcoming Phishing

The "Windows Defender" aspect of Windows 10 is a remarkable antivirus and firewall product, and Microsoft should be given further credit for the manner in which they automatically install patches to overcome vulnerabilities as they are recognised. (Though I wish it would not default to a US keyboard on my computer!)

They are now working on a new container structure that will counter the triggering of a macro which is the manner in which a phishing attack penetrates your computer, we quote:-
"You will be able to open an untrusted Word, Excel, or PowerPoint file in a virtualized container. View, print, edit and save changes to untrusted Office documents - all while benefiting from that same hardware-level security. If the untrusted file is malicious, the attack is contained and the host machine untouched. A new container is created every time you log in, providing a clean start as well as peace of mind."

Of course the criminals will find new ways, but full marks to Microsoft for their continued diligence on our behalf

4 Cyber-attack?

Apparently a prominent political party suffered a serious cyber-attack that originated from Russia or Brazil, possibly both, no data was believed to have been taken.

My goodness, what absolute garbage. We cannot afford to ignore the real risks that are out there, but this was a "denial of service" attack, they can be purchased from the Dark Net for a few pounds. What you buy is an extensive network of infected processor capacity that bombards the target IP address with so much traffic that it is flooded – causing it to slow down or fall over.

Thus it really only has nuisance value, there can be no risk of data exfiltration, and it is totally impossible to define where it came from, there could be literally millions of IP sources involved.

It is disappointing that political drama was allowed to mislead a public that would not know the difference, and even more disappointing to read that the party concerned were not going to change their $20 defence mechanism. Not that it would help with a DDOS attack, but there will be far more professional forces at work, and they will be hoping not to be found, for people not to know they are there.

Two lessons, the first being that the lack of education and understanding of far too many who should know better makes it far too easy for cybercrime to prosper, especially when they fail to adopt counter measures. The other lesson? The truth is that we are yet to learn it. Complacency has been restored, and there will be something going on that we may discover in several months' time, and then we will all be appalled. Last time it was the Facebook fake accounts, with fake news. What will it be this time?

5 Redacting documents using Adobe Pro

A good tip picked up whilst going through a complex subject access request is that any document that is scanned into Adobe Pro can be "redacted" digitally. It was also pointed out that if the entire document is captured in this digital form it can be shared to confirm that no redactions have been missed, and then delivered to the requesting party without having to print out reams of paper

6 Contractual necessity as a basis for processing

This is an extract from a longer document on this subject, it is provided in case the basis is appropriate to be considered. If it is we can go into greater depth.

Contractual necessity is the most appropriate basis when the processing is necessary in order for a product or service to be provided. Essentially, by choosing this basis you are saying 'we can't comply with our side of the contract without this processing'.

This is not a basis to use lightly – it means that the fundamental aspects of your product or service rely on the processing.

For example, you might be unable to complete an order without processing a delivery or home address. However, just because something is included or permitted by a contract doesn't necessarily mean that it is contractually necessary. If you could deliver the product or service without the processing, then the contractual basis is not going to be the most appropriate.

In some cases, the distinction is clear – you need an address in order to deliver the socks a customer bought. However, any further uses of that address, such as using it for sending them marketing materials, will need a different lawful basis.

Similarly, whilst you need the address so you can post the socks, you don't need to know why the customer bought them in order to do that – so you would need a different lawful basis to collect that information.

7 The right to be forgotten

Satswana seeks to share the problem that exists between the European view of data and the US view; you will find some of our argument here

https://www.satswana.com/resource/SatswanaobjectiontoEUUSPrivacyShield.pdf

It has been brought into sharp focus by Google's response to the "right to be forgotten". What they have failed to do is to remove the data. Instead they have introduced what they have called "Geo Blocking" – meaning that you will not see the data if you login from a European server, everybody else can see it.

Shades of the censorship methods used on Chinese networks.

Google's original motto was "don't be evil", now reinvented as "do the right thing". What do you think of this behaviour? They claim that the law does not apply to their users outside the EU, and that viewpoint has been supported by the European Court of Justice. We gather that the argument was that the EU did not wish to be seen to be dictating law to organisations outside their jurisdiction, something US law has no hesitation in doing! Whatever, it means that one ill-considered posting can potentially ruin a person's life forever, all for the commercial benefit of a vast corporate. "Do the right thing"? Huh!

Google are seeking all means to establish a presence in education with attractive products and absolute control of the Android operating system on phones. When considering your choice we do suggest you reflect on what will happen to any data they harvest.

8 Microsoft Teams

We are fans of central collaboration, where people come to the data rather than data being distributed to the edge, and specifically we are looking for a long term replacement to the ubiquitous use of email.

One new solution that is worth a serious look is Microsoft Teams, which is the 365 competition to the capability marketed by Slack – favoured by City traders who spend all their lives watching screens. Video, chat, file share, you name it.

To make this more interesting, please may we tell you the history of Slack? We would not guarantee the accuracy of all the data, but we understand that a proven management of gaming companies persuaded a Silicon Valley VC to invest $250 Million in a new game. They burned their way through around $80 Million before sitting round the table and agreeing that the product was rubbish, and would go nowhere. But hey, the collaborative tool we have developed to discuss these matters internally is pretty cool! So they used the rest of the money to launch Slack!

Microsoft Teams is both a logical copy and inevitable competition, with added benefits – notably with its current integration into Sharepoint, as an example. In the future Satswana believes that the file and data sharing will develop to the point that it will do what MIS suppliers are failing to do, and that is to provide the centralisation of program functions, so that an IT Manager will no longer have to manage multiple databases. They will have a common form in the centre, and then be passed out to the App in whatever form that requires.

Did the games programmers ever think of that?