Consolidation of Update notices from 2018, edited April 2019

Index of contents

A Spring 2018 copy

As part of our service to you as your Data Protection Officer Satswana has pleasure in bringing you the following notes that we trust you will find of interest. Two concern actual breach activity that we have been involved in, and item 6 is a subject that is likely to concern us all until it is more satisfactorily resolved.

1 **Class actions** for data breaches have already started, with The Times reporting that lawyers "will not be subject to the same constraints on resources as government funded data protection authorities." Obvious really that a Regulator that has to fight for funding or levy fines will not have the same clout as a "no win no fee" claim in a court.

2 Recent small breaches remind us that it is **the cover up** that gets you, not the actual breach. Those who "self-report" will probably have a much easier time than those who seek to avoid admitting it. Not least because one is not a story, the other probably becomes one.

3 So what do you do if you find that you have left a **message regarding a pupil on an incorrect telephone number?** And you have an aggressive person criticising you, saying that they have told you twice before that it is the wrong number? Then the Parent who should have been told gets to know that a neighbour has been given sensitive information? Consider please the dangerous nature of phone messages now, because you can never know who is going to play them back, even with the right number. So what message can you leave? "Please call the School", is that enough, or will it cause panic. No clear answer emerges yet, but an issue that is for sure.

4 When things do go wrong, they can escalate horribly. Consider the case of the poor School that suffered when answering a particularly vexatious Subject Access Request, and accidentally sent the document in an envelope that already contained **two pages of parents evening notes**. This was "self-reported" to remove any form of further use that could be made of the mistake by the attacker.

5 We have identified how most telephone systems were developed well before security became such an issue, so you should check vulnerabilities with the supplier, but have you also considered those **devices that record your activity**, Fitbit for instance? Like too many "Internet of things" (IOT) devices (including smart meters) nobody thought at the design stage how they could be used by criminals. Do not allow any users to attach such devices to your network in any way (normally through the USB port that should be "locked down"). If you have to allow any access to any "smart" device to the Internet, it should be on an entirely separate network that has to be monitored to ensure that it does not become part of a Botnet.

6 In the Sunday Times on April 1st there were four letters relevant to the concern we express regarding the limits on data sharing under **GDPR in safeguarding situations**. You will know the name of Sharon Shoesmith as

the former director of children's services in Haringey, and then there was an ex police officer involved in safeguarding in a secondary school whose name was withheld – and the policy manager of the NSPCC. Finally, there was Steve Wood, deputy commissioner at the Information Commissioners Office. Whilst every one of these correspondents implied the word "should", none used the word "must" – indeed most worryingly Steve Wood referred to the Data Protection Act which is due to be repealed. In our understanding a Regulation is the Law and it cannot be countered by "advice", however sensible and logical that might appear to be. To provide clarity for all those involved in safeguarding the law "must" be clear. Until that time issues such as "specific consent" and "the right to be forgotten" create an unintended consequence. NB – update 2019, Keeping children safe in education makes it quite clear that GDPR should never be used as a reason for withholding data in a Safeguarding situation.

B Satswana GDPR Update, information sheet (summer)

1 Admissions forms, lessons learned from other activity

The important point here is to ensure that any Admissions Form, Data capture sheet, or supplementary information form, carries a GDPR compliant statement as soon as possible so that you are gathering consent from new information immediately. You might already have a Data Protection Act statement, we suggest you replace it.

As a guide only, we produced the following form of words for another school – you can adapt as you see fit. "The 'Generic' Academy is compliant with the General Data Protection Regulation which means we seek your specific consent to use the data we are collecting within this Admissions Form (data collection sheet, or supplementary data sheet?) for the purposes as detailed within the Privacy Policy on the School website. We request that you sign this form to confirm that you are giving us your specific consent for the use of this data for the specific purposes outlined only."

Please note that we are suggesting you refer to a privacy policy on your website, which means that the policy must cover all your uses of data, and hopefully our draft will help you there. As a caution, other schools have tried sending out a form with multiple questions and tick boxes with the best of intentions, but very variable results. You start with a distribution issue, do you hand deliver via a pupil, email, or write a letter? You almost certainly know the snags with all three options, but the reality is that you will not get a one hundred percent return.

Then there is the confusion in response, if a box is not ticked have they actually opted out, or misunderstood? Can you have one pupil in a class doing maths homework online, and another not? You know that some of your parents may not be comfortable with filling up a form at all. Thus we suggest the broadest possible

approach, reflecting that there will always be the odd person without access to the website – but we believe that to be the easiest snag to overcome.

2 Seeking revised consent, do you have to?

The Deputy Commissioner of the Information Commissioners Office was interviewed on Radio 4 on Thursday morning where he advised that organisations that had essentially a closed user group did not need to seek fresh consent to continue to contact them. He was actually talking about sports clubs, but local authorities and schools both have a similar fixed "membership". Rather than doing a lot of extra work re-contacting people, a "wait and see" approach might be called for? Certainly you should update your privacy policy, publish it on the website, and use any opportunity to bring the revisions to the attention of your audience. But you can also probably wait and see if anybody objects to being contacted. Make sure please that you do have an "unsubscribe" policy if they do.

3 Class Dojo

It is really worrying to read (The Times, Saturday April 28th, page 4) that Class Dojo is not only storing its data in the US, but also sharing it with 22 third party service providers, including Facebook and Google. The complexities of their terms have been questioned. What we would ask is why a business created by a teacher from the UK is domiciled in the US? They are claiming that they will be GDPR compliant, but see number 4 below. What we all have to challenge is the revenue model that any service organisation has, not just for Class Dojo, but for any app or service that targets any sector. If it is free to use, then almost certainly it is because the data is valuable to somebody else; that is they are harvesting your information and then selling it on. Is that something you are happy with? Who is paying to receive behavioural data from children, and why?

4 GDPR Compliance? Serious challenge required

We are now seeing on a daily basis claims that xyz is compliant with GDPR. In almost every instance, they most passionately are NOT!

To be clear, a statement from a processor is simply not good enough. The data responsibility lies with the controller, and GDPR requires a comprehensive contract between the controller and the processor, in a regulated form. (And if a sub processor is used by the processor; that also requires the same detailed form of contract.) If the information does not include the detail required in the Regulation, then they are not compliant. It is distressing that so many macro organisations have failed to come up with a suitable contract, or in some cases not addressed it at all. There is little an individual controller can do to change that, but we have to stress that the RISK remains with the controller. If you accept bland assurances, and it all goes wrong, then GDPR will hold you liable, not the processor.

Which brings us to the source of a great deal of "fake" compliance namely from the United States, we will explain why we recommend that no assurances should be accepted regarding the storage of any data that is not within the UK or European Union.

Quick history, the US had a privacy law called Safe Harbor that was held to be illegal under the terms of the First Amendment. Now they have something called Privacy Shield, where organisations "self-certify" their compliance. First point, noting what seems to increasingly pass for the morality (sic) of social media organisations, how happy are you with their certifying themselves, do you feel they can be trusted?

But secondly, how are you going to know, and what can you do about it? Candidly we can see no reason why Privacy Shield is not also likely to be challenged under the First Amendment, so it may not be robust law in the first place, but the real question is one of redress. Do you really fancy your chances pursuing an American Company under US law?

If your data is stored in Europe or the UK then you have Regulators in each Country who are all subject to the same law. (Yes, we recognise that Brexit means that we will have a new Data Protection Bill, but it follows GDPR and if you have just one European person within your data, then it will be GDPR that you are subject to. For all reasonable intents and purposes, it is GDPR that is being adopted as good practice internationally, that is everywhere but the US – who are constrained by the aforementioned First Amendment.) So you have a Regulator that will fight a case for you, one that has muscle and power. Why would you seek to walk alone and risk the challenge of US law?

5 Contract

Please note that there are certain places that you must publish who your DPO is, on your website for example. For those purposes the DPO should be Satswana Ltd please, with email of info@satswana.com ; telephone number 01252 516898, if you need an office address as well it is Pembroke House, St Christopher's Place, Farnborough, Hampshire, GU14 0NH.

C Satswana DPO Autumn 2018 Update

Principally this update reviews the problems that we have been dealing with on behalf of customers; please note carefully our comment on retention. We also introduce the new expression of "zero trust" and update you on the NCSC recommendations regarding passwords.

1.0 Problems

We have dealt with a fairly constant stream of issues that we would break down into three categories, the first being bad luck, the second the increasing emergence of subject access requests, and then finally the fortunately few really serious subjects.

1.1 Bad luck

There is an expression that 'you make your own luck' but it really is unfortunate when you have embraced all the recommendations on encryption, and before you can implement them a thief removes tablets, PC's or phones containing data in clear. To date the ICO have responded to all reported breaches with "no further action to be taken" albeit with recommendations to be adopted to prevent a future occurrence. Be aware though that it is not just what you do, but what others do to you that can bite. It can also be classed as bad luck if data is lost, perhaps due to a moment's inattention, the accidental use of the wrong email address, or including data in a file that should not have been provided. The good news is that all these issues were resolved, but not without some anxiety in the first place.

1.2 Subject Access Requests

Together with FOI's, SAR's have (as forecast) become a weapon of choice that we could all do without. Where it involves probing for information by journalists, or similar organisations pursuing an agenda, then there is very little option but to comply. We have had a certain degree of success by seeking to engage with the applicant regarding their interest, and on occasions that has limited the range of documents to be provided, but it does not always work.

Where individuals make the request there is all too often a situation where split families use a demand for information on a child as a means of communication, which may not be possible to comply with if there is a relevant Court Order involved. All Teachers will recognise this as a cry for help, with the associated frustration that would state 'nobody will listen to me'. Suffice it to say that there will be circumstances in which mediation can help, and we have been able to provide that on a few occasions.

1.3 Serious issues

The deliberate and systematic removal of information to a personal archive by a person in a position of trust is misconduct, and very sadly these things do emerge, and then the consequences are significant. That is especially so if some of the data enters the public domain due to the loss of an item where the data is stored. The case may hit the headlines, but until it does, then no more should be said, save to stress that the information belongs to the institution, not the office holder who might manage it. If they cease to hold the position, then their right of access also ceases.

We contemplated putting our final case into the 'bad luck' category, but decided that it was actually an example of almost incomprehensible stupidity, and was thus 'serious'. The subject logged onto a porn site from his personal laptop whilst connected to the organisation network. (Not a school, as it happens!) Remorse followed receipt of an email informing him that they had activated his camera and obtained access to his contact list. Payment of $400 in Bitcoin would halt the otherwise distribution of the film and its circumstances to the contact list. We believed this to be a bluff after establishing that he had disclosed his email address (as a sign on!) and checking access logs. As a precaution his contacts were advised that he had a virus and to ignore any communication from that address. To date, it seems to be contained, and (needless to say) he will never repeat the exercise.

1.4 Retention

You only have to disclose information within an FOI or SAR that you currently hold. Somewhat bizarrely this includes data that may be in a 'deleted items' file. In almost every case we found that no data deletion policy had actually been executed, so organisations had to deliver data going back many years – much of it seriously historical and totally irrelevant. All of the customers we have worked with made sure that they both created a policy and used the summer break to ensure deletion! Thus they will not be caught a second time. All wished they had acted sooner!!

2.0 Zero Trust

This is an emerging concept that involves an architecture that assumes that everything on the network is hostile. Quite how it will be deployed has yet to emerge, but in some senses it is a logical development to the "trust but verify" status that we largely have today – an expression that was originally a Russian proverb. Assuming that everything is bad, until it is re-authenticated, will certainly remove the risk that an unauthorised party might take over your machine. It may be interesting to note that banks are working on artificial intelligence that detects your 'style' in the use and movement of both key strokes and mouse movements – all in the cause of constant authentication.

3.0 Passwords

For detailed information on the latest thinking on the changes that should be applied to passwords, it is best to refer you to the "Oracle" itself, which can be found at https://www.ncsc.gov.uk/articles/problems-forcing-regular-password-expiry

Read here why the constant changing of a password might actually be seen as a weakness, rather than strength.

Once again, real change may emerge slowly, with Microsoft still enforcing quarterly change on their controlled platforms, but we believe the NCSC to be right.

D Update Notice October 2018

In issuing this update notice may we bring to your attention earlier dated notices, advice papers and our Guidance Notes, to be found under the Resources Tab at www.satswana.com . There is specific commentary on NHS vaccinations, Subject Access Requests and the EU/US Privacy Shield that we hope will inform you.

1 A quick GDPR audit check!

a) Have you…..

1 Provided a Privacy Policy on your website
2 Added a GDPR statement to your admissions documents
3 Noted Satswana as your DPO on your website
4 Started a Processor list (see Guide, Appendix D!)
5 Encrypted data wherever possible
6 Considered your retention policy (See main Clause 2 below!)
7 Shredded all redundant paper records
8 Planned a response to a breach (See main clause 3 below)

b) Ensured that Staff have an understanding as follows:-

1 That ownership of data is returned to the individual, together with a right to compensation and a right to be forgotten
2 That they are “not the target” when controlling data, so they should have no fear reporting a breach, even if an accident and/or embarrassing. (It is the cover up that gets you, not the breach.)
3 That work processes will change over the next few years to reduce paper files and favour digital document collaboration.
4 That data should be encrypted, especially where phones are used.

c) Are there any areas of doubt that we can help you with? We are always happy to visit, answer questions by email or discuss on the phone.

2 Retention Policy?

We will have discussed the benefits of deleting data as soon as you possibly can within the landscape that is coloured by Subject Access Requests and the Freedom of Information Act, but there is huge confusion as to what is actually the law, and what is custom and practice that can be changed.

Currently under review is the Information Management Toolkit for Schools produced by the Information and Records Management Society https://irms.org.uk/? And Satswana have sought to contribute to its production. In the meantime V5 dated 2016 is available here https://cdn.ymaws.com/irms.site-

ym.com/resource/collection/8BCEF755-0353-4F66-9877-CCDA4BFEEAC4/2016_IRMS_Toolkit_for_Schools_v5_Master.pdf

It is written with regard to the DPA 1998 rather than GDPR but still has valuable information, though its concentration on a paper file is something we would wish to see radically changed in the next version. We hope to bring you an update as soon as it is published.

Concentrate the mind time? "Be aware that anything you write in an email could potentially be made public!"

E-mail applications are not designed for keeping e-mail as a record. E-mails may need to be saved into any appropriate electronic filing system or printed out and placed on paper files. They can then be safely deleted.

3 Breach (and possibly Disaster) planning?

This is such an easy subject to lose sight of when all is going well, and a tragedy if it is not addressed and something goes wrong. We would like to highlight it in this update notice and ask you to take positive action as follows:-

a) Review all your backup policies for all your data systems and ensure that they are not only being conducted, but that you can also "restore" from them.
b) One of the risks you face is from Ransomware that will encrypt your data (even if it is already encrypted) which makes it inaccessible and unusable. If you do not discover this quickly enough, it can also infect your backups. We advise that once a month you take an "Archive" copy onto an entirely different server location. This then becomes a 'protected' backup that can also be an emergency data source. It cannot be ideal, as you may lose up to one month's updates to the system, but it is a lot better than having no data at all.
c) You must have a management response plan in place in case of a breach, with two essentials. First, a person both nominated and trained to handle the media or any external party with a prepared response script. Secondly a web page that you can instantly mount to inform online queries. (Ask us for help on this if you are uncertain how to go about it.) This must be planned for; you do not have a hope of getting it right by 'winging it'. (Do you recall the chaotic Talk Talk media circus?)
d) It can be disaster as well as a breach that compromises your data; both fire and flood would be a problem for paper records. That is yet another case for digitization where you can send the backup to a remote location.

We know that this is yet another job on a list that seems endless, but ask yourself what if it did happen, and you had not done it? Sorry to nag, but we think it important!

4 CEO Fraud

In closing, and with half term coming up, may we remind you of the perils of CEO Fraud, also known as Business Email Compromise (BEC). The criminal will exploit a holiday period.

By compromising email accounts within a company or institution (normally through a phishing attack), attackers learn, for example, how invoices are paid and can seek to defraud victims based on intimate knowledge of how organizations pay their bills.

It then exploits the trust that will exist between (say) a Head and a Business Manager to send an entirely believable instruction to pay an invoice that the "Head forgot to pay before they went on leave" or some similar line. They will use the language, style and mannerisms that they will have learned from genuine correspondence.

Be very wary of all such instructions. Always confirm them via another route (to e-mail) with the person giving the order. Paying an invoice a week late is never as serious a problem as sending the money to the wrong person!

E Winter Update 2018

1 Capita / SIMS Processor Agreement

This most important document turned up disguised as a "GDPR Contract Variation Annex A" that you may well have been asked to countersign and return, together with a CES Data Retention Statement that is most welcome. We continue to warn that some agreements cannot be relied upon, and there are elements of detail that we could criticise with this one, but it very substantively fits the bill, and when taken in conjunction with their Privacy Statements complies with the GDPR requirement. So for all those SIMS users who have signed and returned the Annex, that is one 'tick' in the box against your data sharing arrangements with Capita and CES.

2 HTTPS?

Standing for 'Hypertext Transfer Protocol Secure' the communication protocol is encrypted, which we all know is good, but the major benefit of ensuring that your website is protected like this is that it provides authentication that it really is you and not an imposter. So it is "a good thing", but as with all such – if you build a higher wall, then the criminal will build a higher ladder. Thus it is no surprise that a "scam" website will also adopt the padlock that signifies that it should be secure – but actually our cyber police ought to be able (over time) to get on top of that, and any threat intelligence service should quickly isolate them. Adopt it please because it represents best practice, and confirms that you are you. Because it is open to abuse is not a reason to stick with insecure and unauthenticated HTTP.

3 Threat Intelligence?

This is not a technical subject, so please do not think it is complicated, it is simple logic. If you get a call from a known criminal, do you speak to them? No, you put the phone down! On the Internet criminals infect your PC with a tiny virus, normally by a 'phishing' attack, and then instruct your machine to call a "command and control" server that then sends a significant load of nastiness. Most Internet Service Providers can identify these 'callers" within about twenty minutes and then add it to a list of people that they will not talk to. So the criminals should be put out of business, right? Well, yes, if it was not for the fact that they are using your PC perhaps as the server, having infected it earlier, or any other number of ways that they survive our defences. Fact is, the further you get away from the really big organisations, then the more time it is going to take to distribute the danger list, and the more it costs to manage. That is one reason why a "cloud" based solution is going to be better in the future; they can afford the resources to implement greater protection. Last quick word, again not technical, so stay with us please, and that is there is an organisation called Dark Trace. Founded by Mathematicians from Cambridge (only in 2013) they use artificial intelligence techniques to predict threats and then build a defence that reacts automatically, without human involvement. How is that possible? Through the use of complex algorithms that are far beyond this writer's understanding. They now have 800 employees and 39 offices globally. Crime pays for some!

4 More breaches in education?

This was a cheap headline, but we do not believe it – more a case of reporting small incidents as a result of the greater awareness surrounding GDPR. Thankfully recent ICO guidance suggests that if there is "no risk to persons" arising from a breach then it need not be reported – though please still tell us as your DPO as insurance and get a confirming email from us that we have considered the case and agree that there is no risk. We suspect that there will be fewer cases as a result next year. (Example of a no risk breach would be accidentally sending an email to a Parent with the same name as a Teacher.)

5 Ofsted go all electronic

We still seek any guidance we can get regarding the Ofsted view of GDPR in an inspection, and were intrigued to note that they are going entirely electronic, which hopefully means that they will be encouraging a significant reduction in paper records. We did note a comment that they will be making sure that all potential information about safeguarding concerns and safeguarding arrangements are properly reviewed, and pupil and parent questionnaires were specifically mentioned. Historically this has been an area where paper files and case notes dominated, whereas the recommended "direction of travel" is to digitise everything in a secure manner.

6 Update to IRMS release date

The question of digitisation brings us to retention policies, notably the update from the Information Records Management Society where we now expect their next release to be available in mid-year 2019. We should all be aware that the work is being done by volunteers who in turn have been busy with their own implementation of GDPR, so we must be patient.

7 Vive la difference, the GDPR or DPA 2018

For a quick appreciation, the DPA 2018 is 354 pages whereas GDPR is an elegant 87 pages, with the first almost 200 pages of DPA being almost exclusively exceptions, amendments and definitions. It is almost certainly regarded as a virtuoso drafting performance, with further exceptions for Scotland and Northern Ireland to add to an impenetrable understanding.

There are two arising points. First, GDPR is the legislation that is being adopted as a world standard, not least because anybody that retains or uses data on a European subject must comply with it. That includes Chinese, Indian, South American etc. territories as well as the UK after Brexit – if you hold data on just one citizen of a European State, you must comply with GDPR. So the second point is that we will still regard European Law as the standard, but in several questions may have to seek to comprehend whether DPA provides an amended interpretation.

In many senses the variations are quite scary, especially in the extension of areas where the State reserves additional powers to itself across a much wider range of fields, with the Secretary of State having untrammeled powers to change almost anything on an executive whim. It is probably comprehensible in the light of the increased danger that is represented by cyber-attacks, the State must have the power to defend, but a reading of the extent of the “powers” that have built up over time certainly concentrates the mind.

A material difference is that in most areas the age of consent for a child is held to be13 instead of 16, though that is further confused with ages in Scotland and there is further definition of 18 applying to child abuse data – with yet another exception that over 18 can apply if the person is deemed at risk. As mentioned above, there may be less easy answers to questions! A Continental child will remain at 16.

Perhaps helpful are exceptions in respect of references, exams, journalistic and academic data from disclosure. When combined with consideration of the University of Worcester decision this is likely to make either an FOI or SAR less of a minefield, with an increased element of executive privilege for data.

Parish Councils, once again in their various defined forms throughout the Country, were excluded from the FOI requirement to employ a DPO.

DPA then goes on through many pages, noting in particular that the DPA 1998 is repealed, and then adding the GDPR derived changes to countless other Acts of Parliament. Who knew that we had a Dentists Act 1984, or an Opticians Act 1989? In any event, they are now all suitably amended. Not to forget the devolved Laws of Scotland, Wales (including text in Welsh) and Northern Ireland!

It is certainly a masterclass in drafting complexity, perhaps reflecting the scale and interaction of legislation that has built up over so many years. But with very few exceptions and variations it gives effect under English Law to GDPR, and we will continue to be guided by that, except when we have to apply a difference!

8 The danger of keys

Your caretaker misplaces a set of master keys, together with an electronic ID card that also gives access to the building – with the name of the School on it. What is the risk and what are the consequences?

Very severe is the answer, quite apart from the chance that somebody will pick them up and then steal data and property from the buildings, how much does it cost to replace all the locks – and provide everybody with replacement keys?

This happened the other day, so in an exercise of slamming stable doors shut, please can we ask you all to consider attaching one of the "key finder" solutions to any set entrusted to anybody within your community. Indeed, is this a thought for anything valuable that identifies you to be secured?

9 Body cameras

G4S may collect money from you, in which case be aware that in future they (and organisations like them) will be wearing body cameras to record evidence in the case of an attack. It is made clear that they are the data controller, that an incident is only stored if there is an attack – otherwise the data is overwritten as they leave the premises – and that the data is encrypted and only readable in the central office.

It was the suggestion of one Council that Parents should be advised of this in your privacy policy, but Satswana does not agree, in that you are not the "controller" – G4S is. Furthermore, we can see an extension of body cameras to a whole range of people, being the Police, Cyclists, delivery drivers etc. We postulate that even Ofsted might decide to adopt them, so where do you stop?

Just possibly we might consider adding a clause to the CCTV policy, to the effect that "Certain contractors with lawful access to the site may record images on a body camera that is only viewed if there is an incident" – does that cover the situation? All views welcome!

