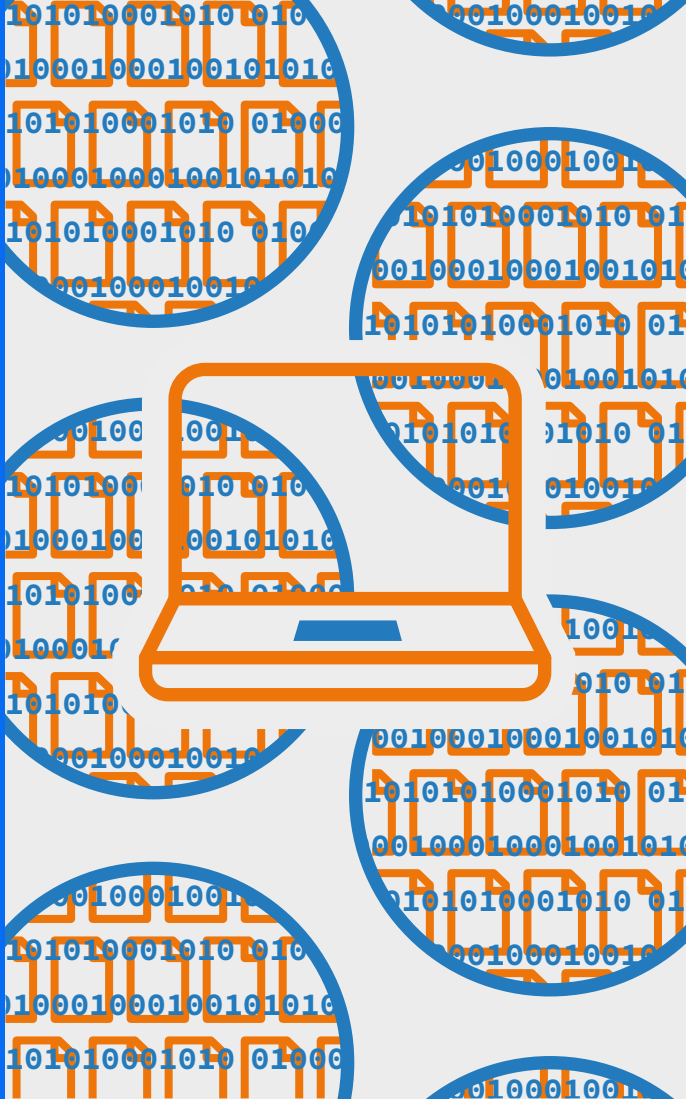
Securys®

Enterprise Insights

Stop hoarding!



Why it is time to ditch that hoarding habit when it comes to data.

Letting go is hard. Who knows whether that washer, or piece of string, or unidentifiable piece of moulded plastic will come in handy one day? Perhaps you will be able to fit into those jeans. Maybe legwarmers will come back into fashion. Most people fail the Marie Kondo test*.

Sadly, many businesses do too. Except that instead of drawers and cupboards filled with items that should have been recycled long ago, they have filing cabinets, SharePoint folders and databases bursting with personal data that they no longer need.

Unfortunately, this is where the analogy breaks down. If, heaven forbid, you were burgled and somebody stole the contents of your junk drawer or the wardrobe in the spare room, you'd probably think it a blessing. But when hackers compromise your network and make off with personal data, real people suffer real harm.

Retention management – the art and science of getting rid of data – is often the neglected Cinderella of data protection, but it's by far the easiest way to reduce your exposure. Information you don't have can't be stolen or misused, and the less data you store the easier it is to organise and protect.

*The Marie Kondo method encourages tidying by category – not by location – beginning with clothes, then moving on to books, papers, komono (miscellaneous items), and, finally, sentimental. items.

When hackers compromise your network and make off with personal data, real people suffer real harm.

Where to start

If you have a data hoarding habit, it can be very difficult to know where to start. Oddly, the easiest thing is often to start with new data: as you collect it, assign it a lifetime and implement a process for getting rid of it. This helps you learn what you do and don't need to keep and get used to the idea of deletion. Once you have the routines in place, you can start applying the same thinking to historic files.

However, sometimes you just have an overwhelming volume of old data – too much to go through in detail. This is where you need to be bold. Don't rely on urban myths about how long you need to retain information – do some proper research into what you are legally required to keep, and for how long. Find those files, put them aside, and then brace yourself and get deleting in bulk.

Remember, too, that retention management isn't just a binary decision. You can delete parts of a file – this is easier with digital than paper, of course. For instance, when an employee leaves you have to retain their payroll information for three years after the end of the tax year (in the UK). But you can remove the employee's bank details as soon as you've paid them for the last time and delete their performance records once the window for an unfair dismissal claim has passed. Be smart and you'll find retention management is less daunting.

Finally, if you can't delete: redact! Sometimes you have to keep even sensitive data for long periods – consider for example passport copies used to evidence the right to work. Documents like this present a real risk to data subjects if they breach – identity theft above all.

Fact here which can be an explanation of something or description of an acronym.

Don't rely on urban myths about how long you need to retain information – do some proper research into what you are legally required to keep, and for how long.

The Securys solution

So, what to do if you must retain them? Use Acrobat or a similar tool to put a watermark across the document that identifies your organisation and the purpose of the document; then no-one else can re-use it. Make sure you save any redacted files with a password to prevent editing, or use “fill and sign” to create a read-only version.

Along the same lines, where you have systems that don’t allow deletion – many HR and payroll systems, for instance, make it very difficult to delete individual records – don’t forget the all-important “x” key on your keyboard. Overwrite sensitive data you no longer need – NI numbers, personal phone numbers, identity document details – if you can’t delete them.

Always think how the personal data you have might be misused in a breach, and work to minimise that possible harm by deleting what you can, redacting what you can’t and encrypting what remains.

Always think how the personal data you have might be misused in a breach.

Find out more

To understand more about how Securys can help you via our outsourced data protection services including DPO-as-a-Service and Assisted Compliance, please contact Stuart Richards at info@securys.co.uk.

For a full list of our services please click here.

About Securys

Securys is a specialist data privacy consultancy with a difference. We're not a law firm, but we employ lawyers. We're not a cybersecurity business but our staff qualifications include CISSP and CISA. We're not selling a one-size-fits-all tech product, but we've built proprietary tools and techniques that work with the class-leading GRC products to simplify and streamline the hardest tasks in assuring privacy.

We're corporate members of the IAPP, and all our consultants are required to obtain one or more IAPP certifications. We're ISO 27001-certified and have a comprehensive set of policies and frameworks to help our clients achieve and maintain certification. Above all our relentless focus is on practical operational delivery of effective data privacy for all your stakeholders.

Securys®
Privacy Made Practical®

161-165 Farringdon Road
London
EC1R 3AL

T 0800 193 8700
E info@securys.co.uk
W www.securys.co.uk

securys-limited
@SecurysUK

UK0013/0122