Simple explanations
Practical check lists and useful links

SECURITY STAFFING GDPR

an AXLR8 eBook

Introduction

Information rights are important to us all. We have laws to protect our data with high penalties for non-compliance, potential damages and reputation loss for any company ignoring the rules.

The damage to your business from GDPR non-compliance could be huge. However, to work in some industries, regulations demand that Staff give up a great deal of detailed private information during the vetting process. Businesses with a vetting requirement must collect the data in systems and keep it secure and be seen to comply with data protection laws.

To make it simple, we have tried to provide both:

- links to the source documents for the details
- simple, practical checklists which your company can plug straight into your policies and procedures.

Who is this document for?

This document is aimed at the management and directors of security staffing companies. Much is relevant for staffing operators in other highly regulated industries such as care staffing, and airside staff agencies.

Security staffing agencies must balance GDPR must obtain and keep information for other reasons, including some statutory requirements:

- SIA and other checks
- ACS and other audits
- HMRC
- Home Office/ Rights to work.
- Employee record keeping and any subject access requests
- Transparency about the reasons why you collect personal data and how you process it.

The industry must collect all this data. High quality systems with a human touch, and clear explanations show that the rules are applied by professional caring people for good people. More importantly, in the event of a data breach or other event, good practice will mitigate or eliminate penalties. Hopefully, this eBook's checklists will help you do that to a high level of quality at the least possible cost to your business.

Who are AXLR8?

AXLR8 have worked with hundreds of professionals and their advisors in the public and private sector and keep up-to-date on this subject. There are complex rules, multiple interpretations and high fines. That means it will cost your management time to comply and you may pay experts to assist and advise.

Hopefully, this eBook can simplify GDPR, and provide practical checklists to help you navigate the seemingly conflicting demands for equality, rights to work, industry regulators.

AXLR8 provide systems for security staffing companies and you can see more information at https://staffing.axlr8.com

Features

- Applicant tracking
- Recruitment
- Right to work
- Automated messaging
- BS 7858 Vetting
- Contract management
- Staff bank management
- Staffing operations and booking shifts for contracts
- Staff App
- Push Messaging
- Texting
- Time and attendance
- Welfare checks
- Lone workers
- E-Learning and training
- Payroll
- Client invoicing
- Managing sub-contractor relationships
- Control room portal
- Client Portal

Please feel free to cut and paste any list to use for checking GDPR for your staff.

The small print:

E&OE: This is a simplified guide. Please check with a lawyer for your own contracts and procedures. If you publish any parts of this internally or externally for any reason, please acknowledge AXLR8 and any other sources we have referenced.

Table of Contents

1. What is GDPR and why should I care?

What is GDPR?

The General Data Protection Regulations took over from the Data Protection Act (1974) in the UK in May 2018.

Why must my business comply?

Organizations should comply with General Data Protection Regulation (GDPR) to protect the privacy of people, avoid fines, and build trust with customers and prospects.

- **Protect privacy**

GDPR protects people's privacy by giving them control over how their personal data is collected, used, and shared.

- **Avoid fines**

Non-compliance with GDPR can result in fines of up to 4% of a company's global turnover or €20 million, whichever is greater.

- **Build trust**

Complying with the GDPR shows that you value and respect your users' rights and personal information.

- **Prevent fraud and cybercrimes**

GDPR puts in place strict security standards to protect against malicious attacks and hacks.

- **Drive data governance**

GDPR helps organizations better understand their data and unlock new use cases for data sharing.

GDPR applies to most personal data, including basic identity information, web data, health and genetic data, biometric data, and more. It gives users eight basic rights, including the right to access, the right to be informed, and the right to be forgotten.

Before looking at any compliance problem from your company's point of view, it often helps to put yourself in the position of the victim of the crime. Forget you are the company owner for a moment. Imagine you are a guard working in a dangerous environment when your boss has not taken reasonable care of the risks. That is the attitude you need with so many people issues. Data protection is one of them. Imagine your customer discovers they can see other people's data on their customer portal. They will be worried about the data they have shared with you. The matter of lax data protection is becoming inexcusable. This does not just apply to data protection. There are historical parallels with the way attitudes have been changed to wearing car

seatbelts, smoking, drink driving, health and safety at events or workplaces and many other responsibilities we have as business managers and as individuals.

Penalties

Our personal data is protected by law. The financial penalties for companies can be very high for breaking the law and you will be caught as there are a host of people who will report your business. **The fines are a percentage of your profit or turnover for the year. There are examples of fines of hundreds of thousands or Euros/Sterling. This fine is in addition to any financial claims by the data subjects who may have a case for damages**. The TalkTalk £400,000 example of 2016 was well reported in the legal, IT specialist press as well as hitting national news.

Clients have also told us of additional fines from their professional bodies for (e.g.) losing laptops with personal data stored on them.

Damages

In addition to fines, there are damages that may be sought by individuals or organisations. For example, twenty years ago and AXLR8 consultant was on site at an organisation who had released a photo to the press without explicit permission and a remote police force were demanding over half a million pounds for a subsequent witness protection move.

Individual rights

Individual rights from the ICO website (https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-sharing/data-sharing-a-code-of-practice/the-rights-of-individuals/) latest EU updates source here https://www.edps.europa.eu/data-protection/our-work/subjects/rights-individual_en#:~:text=The%20GDPR%20has%20a%20chapter,decision%20based%20solely%20on%20automated

- the right to access personal data held about them (the right of subject access)
- the right to be informed about how and why their data is used - and you must give them privacy information
- the rights to have their data rectified, erased or restricted
- the right to object
- the right to portability of their data
- the right not to be subject to a decision based solely on automated processing

Summary

Businesses hold personal data on their staff which may be used by criminals to commit crimes against those people. You are responsible for keeping that data safe. The financial and reputational penalties for your business can be great.

What must my company do?

There are 7 broad legal principles:

- Lawfulness, fairness and transparency.
- Purpose limitation.
- Data minimisation.
- Accuracy.
- Storage limitation.
- Integrity and confidentiality (security)
- Accountability.

We will apply these in the practical checklists later. First let us review definitions of some important terms.

GDPR Definitions

TERM	DEFINITION, NOTES & CLARIFICATION EXAMPLES
GDPR	General Data Protection Regulations entered UK Law in May 2018
DPA	This normally means the Data Protection Act of 1974 with any amendments up until it was superseded by GDPR in May 2018
DATA PROTECTION	In general terms this applies to the responsibility you take and the care, and secure private storage you provide for the data provided about individuals.
PERSONAL DATA	Any data that can be related to "an identified or identifiable natural person" who can be directly or indirectly identified using it. Some are obvious such as: names, ID numbers, phone numbers, or email addresses. However, some are less obvious like IP addresses, information collected via browser cookies. Some items are very sensitive personal details like gender, religious beliefs, or political affiliation or cause a risk for the individual financially such as banking or credit card details.
SECURITY THREATS	These break down into two very broad categories: your staff and internal system security, and the Data Processor's security
INTERNAL SECURITY	You must maintain secure procedures and systems as the Data Controller (definition below). That includes making sure your staff use secure procedures to protect private data but also checking and agreeing standards with your Data Processor
BIO METRIC ID DATA	Certain unique data such as fingerprints, faces and retinal patterns may be stored digitally and provide matching to each individual.
PII	Often used as an alternative to Personal Data, this term represents information that can be used on its own or with other information to identify, contact, or locate a single person, or to identify an individual. For example, a first name and date of birth can normally narrow down a search in a large population with just a few other data points needed to uniquely identify the person.
CYBER ESSENTIALS	This, and its more strictly tested "Cyber Essentials Plus", are UK standards of data security and you should consider putting your business through them with an auditor.
PRIVACY POLICY	This is a statement that all companies require and we provide an example for you to use in security staffing.

	Briefly, it will list the data you collect, the reasons why and how long you will keep the data and what you do with it.
EMPLOYMENT AGREEMENT	Your employees will be subject to a contract of employment and the reason it is defined in this context is that there are many reasonable statements they should agree to including media rights, the conditions under which they must respond to communications and whether they may unsubscribe to legitimate business communications, etc.
DATA CONTROLLER (DC)	Your company is the Data Controller. The director(s) are responsible for keeping the staff data safe, ensuring your DP (see below) is security accredited and has procedures in place for breaches, that you have contractual agreement about responsibilities, that the staff understand and agree how you hold their data and what to do if there is a problem. Your company (as the DC) is responsible for ensuring that the data is deleted when it is not held according to your retention policy.
DATA PROCESSOR (DP)	This is an outsourced systems company (like AXLR8) handling your data. Your SaaS supplier is the Data Processor (or DP for short). You are responsible for ensuring they process your staff data securely and are compliant with GDPR. NB You are the Data Processor as well as being the Data Controller if you use an in-house system based on your internal server or spreadsheets on employees' PCs and other personal productivity devices and office tools.
LOCATION OF DATA PROCESSING	Right now, it is legal to have your data processed in the UK or the 27 countries of the European Union. The regulations remained aligned after Brexit. However, most suppliers will comply and move clients' server platforms if that should ever change. You may not have your staff details or any other personal data stored or processed in other locations. To be clear, you may not have data stored in e.g. USA, Asia, South America, Russia or Australia. That includes your PC or a developer from your SaaS supplier or anyone analysing or working with personal data from your server in the UK downloaded to their machine.
PRIVATE PERSONAL DATA	This is data about people that must not be shared outside your organisation unless specifically agreed and on reasonable grounds. (see Data Sharing Agreement and Privacy Policy). Apart from PII (above) there is a great deal of personal data held by staffing companies.
DATA SHARING	You may share data with other organisations and you need to list which for staff and why (a) so they know

	where their data is going and agree (e.g. HMRC, clients where they are working in site, subcontractors) and (b) so that you can educate your staff on their responsibilities when accessing data.
DATA SHARING AGREEMENT	This is a signed agreement between two parties about the conditions under which they share data. It is defined in law when dealing with HMRC or Home Office audits or the SIA. However, but the data shared with customers, subcontractors and marketing agencies and your team leaders needs consideration and negotiation. Your office admin staff need to know clear conditions under which they may share data with outside parties.
RETENTION POLICY	How long do you keep certain types of data? This must be stated in your privacy policy and you need to inform office staff and, if automated deletions are processing records beyond the retention period, then you need to brief your Data Processor.
RIGHTS OF AN INDIVIDUAL UNDER GDPR	We all have the following rights and can request that any DC complies with them in a reasonable period of time subject to statutory exceptions (see below) and that we can prove our ID when asking on behalf of ourselves. You might need further proof to ask for information held about a third party. A relevant example here would be employment reference requests.
GREY IT	Systems such as spreadsheets and Whatsapp lists used for productivity, tactical or interim tasks or other reasons by staff. Often unknown but sometimes sanction these are difficult to control and hence multiply your risks of breaching GDPR.
DESTRUCTION LOG	A log of data deleted without PII. For example, a record of the staff ID numbers that have been deleted but no associated PII with which to link them to emails telephone numbers or any other personal private data.
SUBJECT ACCESS REQUEST (SAR)	Any of us, as individuals, may make a (SAR) subject access request for the following.
ACCESS	This right allows us to ask for any information held about us on a database. Beware, this could mean poor personal comments and so you admin staff must be trained and any HR notes or dropdown values must be moderated and reviewed. Assume the staffer will see it. Also relevant here is the right for staff to request accurate 5 year employment history from HMRC.
ERASURE	The DC (your company) may be asked by a staffer to delete all their data. Please note this is different to auto deletion where your Retention Policy states that

	data is deleted at set periods because the promises in your Privacy Policy state that it is no longer reasonably held. This raises many issues. For example: if you wish to retain a record about their employment termination about how you would gladly rehire them or must not re-employ them. Likewise, see exceptions to do with pay, below)
RECTIFICATION	An individual may ask the DC to correct data about themselves. Most staff apps these days allow their staff to see and change most details about themselves.
PORTABILITY	We all have the right to ask for our data to be passed from one organisation to another. This is helpful if your account moves from one bank to another. How it affects a staff agency is less obvious.
RE-USE	As above, it may be that a staff member wants their data, not just human readable but would like an electronic copy like a CSV file in order that they may reuse it. This can also help companies in any highly regulated industry. For example, tax authorities must comply with an individual's request for their five years employment information. (See this example for HMRC as an example in UK)
RESTRICTION	People may allow you to use their data for bookings but not for, say, using their picture for advertising your services.
AUTOMATION	This is the right not to be subject to automated decision-making. For example, are you starting to use algorithms for selecting staff for work or for rejecting applications from candidates?
THE RIGHT TO BE INFORMED	This means telling staff when you make changes.
STATUTORY EXCEPTIONS	An individual may be refused on occasion when requesting the above. For example, most tax authorities have a right to audit your books up to a statutory limit. As an example, this is commonly six years where you need to keep payments, expenses, NI numbers and other records. Likewise, you may have obtained agreement from all staff that they may not unsubscribe, during employment, from communications about work opportunities and future shifts, etc. Likewise, you should have a media clause stating that you can use any promotional material using their image or statements in perpetuity for marketing on your site or other social media. If there are outstanding issues with pay or, if a client record, with payments, it is clear and reasonable that

	you need to retain those records for a period necessary to close the matter.
DISCRIMINATION, EQUALITY AND DIVERSITY	The questions you can ask an applicant or internal candidate must not discriminate against anyone or allow assessors to show bias on an illegal basis. This related subject (what you may ask candidates and employees) is a big subject. We have discussed elsewhere. https://staffing.axlr8.com/go-applicant-blind-for-diversity/. For now, for UK companies, here is a government reference https://www.gov.uk/employer-preventing-discrimination/recruitment. Do not confuse the stage at which you may ask for someone's date of birth or a head shot photo with the requirement under GDPR only to hold it for some legitimate cause and whether anyone selecting for a position may see it and when it should be deleted.

How does it affect my Security staffing agency

It is not about setting the high professional standards we all plan for our business from day one. There are high fines and other penalties for non-compliance and poorly managed data security and privacy soon become visible to clients and staff.

Your business image, reputation and finances can be damaged if you do not comply with the legislation and the spirit of the law. You have to collect private data about guards, door managers and other staff and need to protect it as if it were your own.

Non-Compliance

What are the implications of non-compliance with GDPR?

1. Reputation
2. Fraud
3. lost customers and staff
4. Fines
5. Staff trust
6. Potential effects on other compliance like SIA
7. Wider computer security vulnerability
8. Data theft

In Part 2. We will look at what needs to be done and in Part 3. How to do it effectively and tips to reduce the costs of compliance by "working smart".

2. How should I organize my company to be GDPR compliant?

Education starting at the top.

You should read up about it from the source materials and study online articles for comparisons. Only then can you

- assess threats to your business from the regulator or reputational risks
- trust your judgements about what is required
- train your staff on GDPR

Identify risk areas

Your company will be collecting and storing personal data during many processes. At each stage you will need to define the data that is necessary at that stage and avoid collecting more than is needed. Also, you will need to lock down who is allowed to access different data so that they can only see what is necessary for their job. This is not just a GDPR issue. It is relevant in other area such as avoiding access to data that could allow accusations of discrimination.

Recruitment process

This is dealt with in detail later but the key points are

- collect only that data from he individual that is required for any stage of your recruitment process.
- Tell them exactly what you will collect and why, what you will us it for and how long you will keep it before they start filling out the form.

An example of a "Privacy agreement" for you to use is included here. Feel free to copy and edit for your agency.

This link on discrimination law may be helpful for building good practice into your recruitment processes.

Vetting process

Depending upon your regulator (SIA assumed here) and auditor, you need to see originals of PoID and PoA and scan and record them as the basis for BS7858 vetting.

Once the candidates are showing you original documents in your vetting workshops, you will probably collect other data from uniform size to checking DBS and driving licence if relevant to the work (in addition to being a Class A PoID). You also need evidence of their right to work.

Then you will be obtaining documents and proof from the other areas (residential history, employment history and any qualifications/certificates.)

Booking work shifts

There are many issues where private data may be leaked here. You should avoid giving staff data away as part of the logistics process. Avoid the use Whatsapp groups or email CC lists for groups because they will see all the other people's contact details. Your system should send out individual emails. The staff portal app should contain all they need for work bookings, confirmations, details of Use you company private messaging system where staff cannot see each other's numbers on the app but can communicate, e.g. lift shares, adjustments for late or early arrivals, etc.

Monitoring workers

This link from ICO provides detail. Remember, monitoring workers needs to work for both the legal restrictions under Human Rights law and also the duty of care employers have under health and safety law. There is plenty of space to navigate between the different regulations but you must inform employees and explain clearly what your policies are. This should be

- defined clearly in the employment contract and
- also summarised on your website recruitment area
- included in any deeper training and materials on your induction courses and staff portal/app for confirmation.

https://ico.org.uk/media/for-organisations/uk-gdpr-guidance-and-resources/employment-information/employment-practices-and-data-protection-monitoring-workers-1-0.pdf

Time and attendance

This includes Check-in and Check-out and other geolocation and biometric. QR/ NFC etc. access and guard tour/key systems (not forgetting CCTV)

A business must decide what the minimum period for data retention is for the purposes of collecting cash from customers, paying staff and subcontractors for work, dealing with disputes and audit. Additionally, welfare checks and incident reports need to be available for audit for a period long after the shifts/events. These periods must be agreed in advance with your clients and with staff. Luckily, HMRC statute of limitation mandates/allows you to keep financial information retention for a period of 6 years.

Notes recorded about staff

This is an important matter that could have been included in several sections of this document. If you ask your admin people to write notes on staff, you need to be clear on what the purpose and have a policy. We have had instances where a member of staff has seen what the head office staff booking team have written in the notes and the result was costly for our client in many ways.

Feel free to cut and paste the words below into your policies.

When recording notes on a staff member's details, be careful to stick to facts and avoid opinions and slurs on their record. Any staff member has the right to see their file under GDPR.

There is less risk (not zero) in accurate description of behaviour "Jane was late for her shift and I gave her a second warning and explained the implications for disabled and other visitors if she is not at her post on time".

There should be no subjective opinions on a member of staff that are just insulting even if you have your own opinions about the individual. Also, if you feel that she is a lovely person to deal with and always happy and charming on the 'phone, make sure that it is either not recorded in a way that allows later accusations of discrimination against some other group or of some bias or attraction towards that individual.

If it is important to monitor staff behaviour in customer facing roles, have objective scales and allowed phrases as much as possible. Describe behavioural facts.

Procedures

The principles of GDPR are mostly clear by now. What a business should actually do is discussed in part 3.

Checklists

This is a super list (https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/individual-rights/individual-rights/right-to-be-informed/) from the UK ICO. It is also a rather good checklist for most jurisdictions including EU and US.

What to provide

We provide individuals with all the following privacy information:

☐ The name and contact details of our organisation.

☐ The name and contact details of our representative (if applicable).

☐ The contact details of our data protection officer (if applicable).

☐ The purposes of the processing.

☐ The lawful basis for the processing.

☐ The legitimate interests for the processing (if applicable).

☐ The categories of personal data obtained (if the personal data is not obtained from the individual it relates to).

☐ The recipients or categories of recipients of the personal data.

☐ The details of transfers of the personal data to any third countries or international organisations (if applicable).

☐ The retention periods for the personal data.

☐ The rights available to individuals in respect of the processing.

☐ The right to withdraw consent (if applicable).

☐ The right to lodge a complaint with a supervisory authority.

☐ The source of the personal data (if the personal data is not obtained from the individual it relates to).

☐ The details of whether individuals are under a statutory or contractual obligation to provide the personal data (if applicable, and if the personal data is collected from the individual it relates to).

☐ The details of the existence of automated decision-making, including profiling (if applicable).

When to provide it

☐ We provide individuals with privacy information at the time we collect their personal data from them.

☐ If we obtain personal data from a source other than the individual it relates to, we provide them with privacy information:

☐ within a reasonable period of obtaining the personal data and no later than one month;

☐ if we plan to communicate with the individual, at the latest, when the first communication takes place; or

☐ if we plan to disclose the data to someone else, at the latest, when the data is disclosed.

How to provide it

We provide the information in a way that is:

☐ concise;

☐ transparent;

☐ intelligible;

☐ easily accessible; and

☐ uses clear and plain language.

Changes to the information

☐ We regularly review and, where necessary, update our privacy information.

☐ If we plan to use personal data for a new purpose, we update our privacy information and communicate the changes to individuals before starting any new processing.

Best practice – drafting the information

☐ We undertake an information audit to find out what personal data we hold and what we do with it.

☐ We put ourselves in the position of the people we're collecting information about.

☐ We carry out user testing to evaluate how effective our privacy information is.

Best practice – delivering the information

When providing our privacy information to individuals, we use a combination of appropriate techniques, such as:

☐ a layered approach;

☐ dashboards;

☐ just-in-time notices;

☐ icons; and

☐ mobile and smart device functionalities.

Expert advice

It is tough to choose an advisor. Many self-proclaimed experts are not what they say and often do not agree with each other.

AXLR8 cannot offer consulting services as we are not lawyers. Most lawyers I discuss this subject with admit they are not experts. AXLR8 have provided systems to Information Governance officers for more than 20 years and so have several mentors

we trust. Some have been kind enough to bounce ideas around and help test whether something holds water. I learn something new every day from them.

We can only suggest the obvious criteria:

1. qualifications / accreditations
2. contractual guarantees for their work backed up by solid Professional Indemnity Insurance (PII)
3. Pre-existing model templates and procedures to save you costs and time – perhaps a regular update service.
4. references from other companies in your sector.

The first includes qualified lawyers. A practicing lawyer will also have PII in place and should only take on work where they feel it is within their competence. Specific accreditations would also include IAPP such as the Certified Information Privacy Manager (CIPM). Probably, an HR professional with CIPD will have good knowledge of the area and how it interacts with other regulatory frameworks such as equalities and human rights law.

The last one is interesting. Are they popular with peers because they cut corners or because they are really strict and the people are recommending them because they felt comfortable their process were watertight afterwards.

The area is complex and so one can forgive different experts for occasionally providing advice that seemingly conflicts with other experts.

Staff Training

You must train your office staff what information they may divulge to whom. That means sharing the privacy policy and the related employment contracts and explaining your procedures. Make sure they know and understand how to use their systems and know your current data sharing agreements.

Policies in place

Privacy Policy

Make sure you have a retention policy and that your SaaS supplier automates it. If you are working on spreadsheets, reduce copies and share only with a small trusted number of individuals. Make sure you have a Privacy Agreement signed by applicants before they give you information about themselves which states what data you will hold about them and collect from them at various stages and how long you will hold it, what you will use it for and your reasons. There are lots of points in any regulated industry particularly the security staffing business, so contact AXLR8 if you would like to start with a copy of our model "AXLR8 Security company starter privacy policy".

Do not forget that you must explain to your staff what their responsibilities are. Apart from being truthful and complete in their applications, you need to take elements of this forward into their employment contract.

Employment Contract

Your employment contracts for PAYE staff and self-employed subcontractors will evolve as the business learns and staff behaviours.

You should at the very least add the following if they are not there already.

5. Confirm which data you hold and why and what you will do with it (refer them back to the privacy policy)
6. What to do if they feel there may have been a breach.
7. Their responsibilities e.g. confidentiality of other staff data and your confidential business information, of course about customers and procedures, etc.) This includes never giving away their password and never asking another member of staff for theirs.
8. Media rights over any video, pictures, etc. that you use to market your services and by extension obtain more employment opportunities for them

WhatsApp

Be careful of this tool. It has its advantages, and is easy to use and popular. In fact, it is great! However, be aware that the highest fines (JPMorgan fined $200 million for letting workers use WhatsApp to evade regulators (cnbc.com)) that have been handed out to businesses by regulators concern WhatsApp and that is before you even get to the reputational loss for governments and police forces brought upon them by individuals in WhatsApp groups

We have many case studies of WhatsApp getting staffing companies into trouble See here (https://staffing.axlr8.com/staffing-companies-should-use-watsapp-with-care/).

Just as one example, imagine you set up a WhatsApp group with twenty staff on it. That means you have given every individual the cell phone number of 19 other individuals. In several cases we have heard of, a company has given away their entire vetted security staff contact list and it was stolen and abused at a busy time of year by a direct competitor!

This threat is even worse with spreadsheets. See also “grey IT” section, below.

Can I avoid GDPR?

No. We all have a responsibility to protect people’s data as company managers (and as individuals). Ultimate responsibility lies at the feet of the directors. You need to get legal advice if you are a senior manager who is not listed as a director at Companies House but still have certain systems administration responsibilities.

3. Practical Plans for achieving GDPR compliance

How do I assign responsibility for this and check it is being done.

As a director, you bear the ultimate responsibility. However, you can delegate the tasks and diarise times throughout the year to check the processes are working.

1. Delegate the management to a team member – probably your recruitment and vetting manager. Write the procedures and KPIs into their job objectives and appraisals
2. Train all staff on the processes and explain the policies to all candidates.
3. Automate the tasks as much as possible – see section below. This reduces errors and enforces your data retention policy.
4. Check regularly that nothing is slipping through the net.
5. Record those checks with dates and results. That way, if something ever goes wrong, you have an audit trail showing due care has been taken. This will help your case in any external review.
6. Stop copies of the data multiplying in spreadsheets, whatsapps and text lists. Do it through a centralised system.

What GDPR mistakes should Security Staffing agencies avoid at all costs?

1. Don't ignore GDPR. Apart from the fines, the reputational damage has added to the list of things people really look down upon like smoking, not putting your hand over your mouth when sneezing or coughing or driving after drinking alcohol.
2. Documentation such as policies and procedures missing or incomplete. If nothing else, take the free checklists and documentation we have provided and tune it to your agency.
3. Not checking all is running well.
4. Not responding promptly to SARs even if they are from disgruntled ex-employees.
5. Ignoring Data Breach Reports and whistle blowers
6. not investigating reports of breaches quickly enough
7. Do not miss out on opportunities to automate deletion processes. If you have a "retention period" for a certain type of data of 10 days or one year for another type, then automate the deletions. Do not expect a manager to do it manually. It is what systems are for.
8. Multiple copies of data in "grey IT" – especially spreadsheets and phones (e.g. Whatsapp lists)

Grey IT Risks and costs

Make sure you do not have multiple versions of the database of staff in "grey IT". That means clamp down on any spreadsheets duplicating data on your office PCs and people's other devices. Your SaaS system should be the only system people use. If they are using tactical spreadsheets then there may be a training issue or the supplier should write code to make them redundant. Team leaders should have access to team sheets but not on lots of spreadsheets increasing your GDPR risk.

In rare occasions where a spreadsheet has to be used as an interim (checking and cleaning data before a migration or data sharing are examples), then the data should be logged out and deleted. The deletion after the task for which it was exported should be logged in you destruction logs.

Exceptions

There are a few broad exceptions to accepted GDPR processes that you should agree with your staff.

Exceptions to deletions

1. Bookings
2. Outstanding incidents or enquiries
3. Audit for ACS, HMRC, etc
4. Subcontractor commission relationships
5. Ongoing disputes
6. Commissions payable
7. Holiday pay owing
8. Pay or expenses
9. *Pictures, videos, etc used in marketing or social media on your site or any other

*Would need to be agreed in a media rights section of your *privacy agreement* and your *employment contract*.

Processes

Here are some processes you should document and train your staff about. Check their understanding regularly with quizzes. Most AXLR8 packages have the e-learning platform included so, if you are an AXLR8 client, it is free to write quizzes for staff on these and all your company standards and policies. If you are not an AXLR8 client, there are tools available from spreadsheets to specialist products to do this.

Logging SARs

Have a book or system for logging SARs and make sure they are taken through to completion – a bit like an accident book. Allocate one of your staff to see the process through.

If you have AXLR8, the answer is probably that they can see all their data on your (AXLR8 Staff) staffing app. If your system does not allow this, ask your supplier to export it for a fee. Do not delay more than the statutory calendar month allowed for SARs. If it is a deletion request, remember you need to have agreed in the privacy policy and the employment contract, what data you will retain for statutory reasons (e.g. HMRC) for a longer period.

Recording and reporting Breaches

These should be rare if you attend to security. It is unlikely if you have an established SaaS supplier. If you have an office with spreadsheets on every screen, being passed around between staff, then it is much more likely. Do not ignore them.

Preparing for Data Breaches

After all the security and staff training to prevent data breaches be prepared for one. This preparation will repay you 100% if one occurs.

- Name a team who will look into it. For example,
    - a board director with the legal and IT skills to manage the situation,
    - a representative from your SaaS supplier who holds the data.
    - Possibly the ICT/Network support company but they may be less familiar with your actual data.
    - Your system super user(s) and
    - Hold one or two slots open for a line manager as appropriate
- Have a prepared written policy (Don't worry we have included checklists here for you to copy and paste
- Train your staff on how your data breach procedure works and make sure the messaging encourages whistleblowers.
- Put "slugs" in your data which tell you if it has been leaked or stolen. For example, false names mobiles and emails that are forwarded to you if anyone tries to email your staff or clients. If you change them now and again, you can tell when the data was stolen.
- Define people's responsibilities for data privacy in their job contracts.

Dealing with a Data Breach

It is essential to log data breach reports and put in place a procedure to:

a. Acknowledge the report to the person who informed you and the procedure you will follow.
b. Inform your Data Processor (AXLR8 if you are a client of ours)

c. Perform an initial investigation
d. Make an initial internal response i.e.
    i. We looked into it and are sure it is **not** a breach
    ii. **Yes. It is a breach** and this is what we are doing next
    iii. **Don't know:** there are situations where it is not obvious if a breach has occurred or not[1].

Assuming it is a breach where information has been leaked or stolen, investigation will become expensive and time consuming and you must

e. inform the Information Commissioner for your jurisdiction of the nature of the breach and the personal data that has been exposed.

As with all compliance issues, prevention is better than cure. Good policies internally e.g. Cyber Essentials Plus, standards like ISO27001 and professional SaaS suppliers are the best way to avoid expensive GDPR breaches.

Automation

The "promises" you make in your privacy and employment agreements about how you collect, process and dispose of data will benefit by being automated. This will save your company money and staff boredom leading to mistakes.

Apart from relieving administrative burden for this vigilance task, the automation has many other advantages including

- it forces you to document the retention policy
- the process goes on 24/7 without taking a holiday or going sick
- saves money and time of a senior manager
- staff are less likely to make mistakes.
- Can be set to automate destruction logs as well.

[1] As an example, your SaaS supplier may report they have found suspicious activity on their platform and are investigating. The server has been breached but there is no evidence of any data leakage. These matters are very frustrating and not uncommon. As another more common example, a guard claims there has been a breach because someone obtained his NI number or some other data item. However, this may then turn out to be a breach in another company's system or the guard may have given it away in some other way.

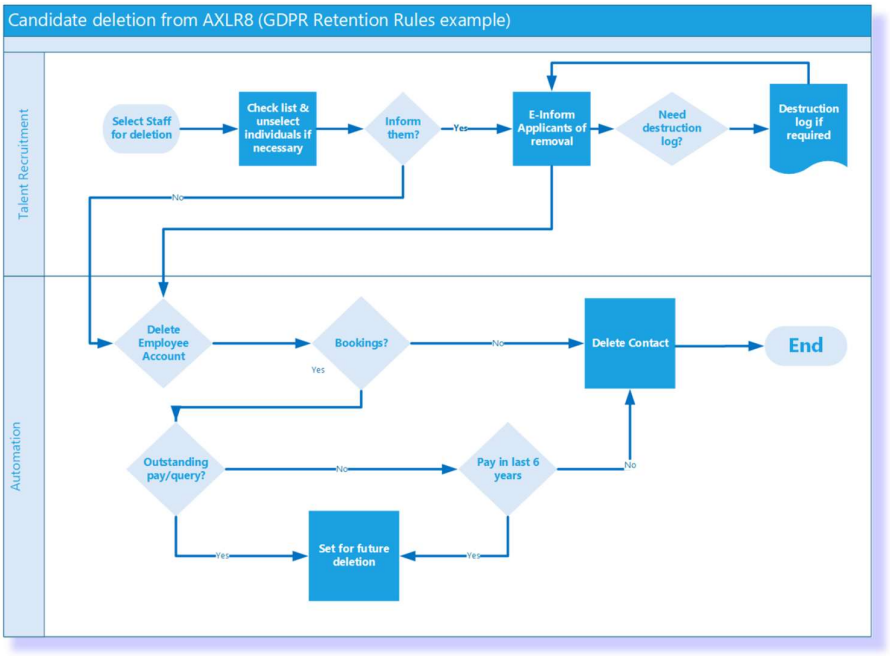
Deletion automation

You may have a policy of deleting staff as follows:

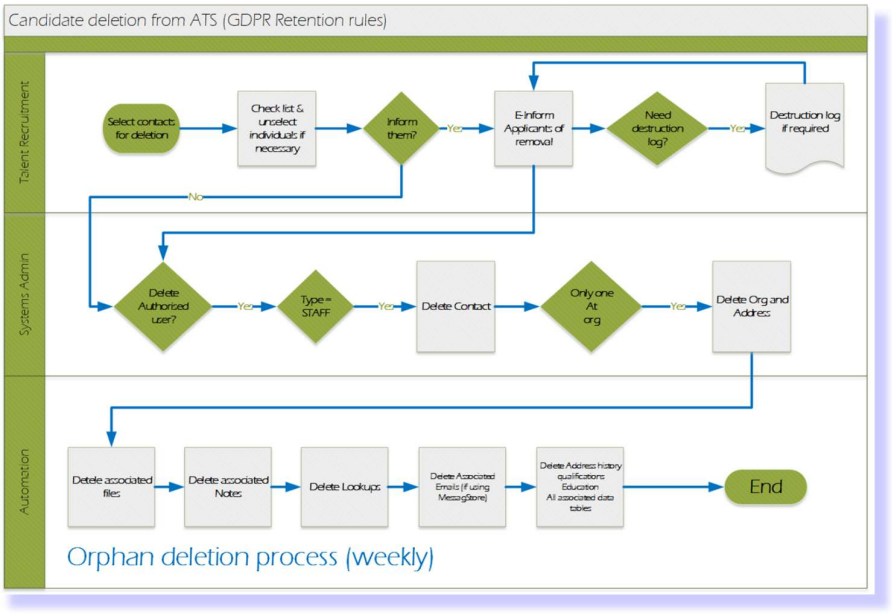
Suggested GDPR Deletion rules for Employment Lifecycle Stage (aka JAS or job application stage in AXLR8).

EMPLOYMENT LIFECYCLE STAGE (JAS)	MESSAGE TIMING	SUMMARY OF AUTO MESSAGE	ADD RECORDS TO WEEKLY AUTO DELETION
STARTED ON THEIR APPLICATION FORM	24 and 72 hours	Reminder to complete and warning they will need to start again.	After about a week or ten days
COMPLETED APPLICATION	Within a few minutes of completion	Thank you and reminder of reasons for gathering that information and what you will use it for	
ADDED TO STAFF BANK BUT NOT EVER BOOKED ON A SHIFT		Ask for permission to keep their details on record for a reasonable period if seasonal work	A few months or up to 2 years in a seasonal business?
BOOKED ON SHIFTS AND WORKED AND WERE PAID			6 years (HMRC)

Sometimes it helps to see this as a flowchart. Here is a generalised auto-deletion flowchart. AXLR8 customise this for different clients. However, this is a good logic flow you and take and customise for your company.



Then, behind the scenes AXLR8 remove associated data on a weekly cycle as shown below. This will be less relevant for non-AXLR8 users but you can use it to see if you have missed any dependencies in autodeletions you build on your system.



Generalised Employment lifecycle stages

The lifecycle an employee goes through stages. You need different rules for autodeletion at different stages. Your company may have names for these stages.

Here are some examples of these job application or lifecycle stages. Where the right-hand column is sparse it is assumed the "Status" column wording is self-explanatory.

STATUS	DESCRIPTION
CONTACT CREATED	Started application form but not yet completed. The more regulated the industry the more documentation and information is necessary for background and other checks. A large proportion of people get distracted before completing their online form. Many systems can be set up to send automatic reminders to those applicants with a set period before partial applications are deleted.
APPLIED	Completed Application form
INVITED TO INTERVIEW	Progressing candidate
REJECTED	Or whatever your word is for "unsuccessful" candidates on this occasion.
ATTENDED INTERVIEW (AKA "STARTED VETTING")	Can work for you for 12 weeks assuming they pass the interview and all R2W and SIA and other documentation are in place
DID NOT MAKE INTERVIEW	You invited them but they did not make it for some reason
REJECTED AT INTERVIEW	You interviewed them but there was an issue or there was not a position for them
ACCEPTED AND READY FOR SHIFTS	Vetting complete and added to registered staff bank
BOOKED ON SOME SHIFTS	They have been offered and have accepted shifts
PAID FOR SHIFTS	Immediately, you need to be sure you can provide HMRC with data for six years.
VETTING COMPLETED	BS7858 vetting completed in the 12 weeks.
TERMINATION WOULD RE-EMPLOY	A term which carries the message that this was a good member of staff without having to say so.
SABBATICAL	Just not available for work for a period. Implied "would re-employ" AKA "Travelling", "Studying" etc.
TERMINATION WOULD NOT RE-EMPLOY	A term with a clear message. It avoids any negative descriptions yet protects your company from re-hiring a potentially disruptive, violent, dishonest ex-staffer.

There will be several other status labels you use in your company and your auto-deletion mechanisms need to deal with those as well. For example, failed Vetting, suspended pending investigation, etc.

In AXLR8 systems, we call these JAS (Job Application Stages). You can change their names as your company and recruitment journey requires.

If you do not use AXLR8, then your chosen systems will be able to advise you about configuring auto deletion for each stage. Hopefully the logic diagram above will be helpful. A retention period for an applicant who has not completed the application form after a couple of auto reminders should probably be deleted after 10-14 days with an auto email explaining this action to them. A staffer who has worked for you and been paid will need data pertaining to pay held for six years. If you have obtained media rights to, say, pictures of them at events or on contracts for marketing purposes, you can keep them, too. You must have a reasonable explanation for this in both

- your privacy agreement (example above you can download and use) and
- your employment agreement.

Autodeletion vs manual deletion costs

If you have a few thousand people on your staff bank, then trying to do auto deletions manually may lead to mistakes. By definition, a GDPR deletion is unrecoverable. A mistake can be very costly. It is worth paying to set up the autodeletion rules for your business and having them tested and maintained by your system supplier and signed off by your SMT.

Lastly, it will also become a vigilance task for a senior trained person in talent management and that is a cost to the business.

4. Comments and feedback

We welcome comments, correction, feedback of any kind.

support@axlr8.com

01344 776500