



## Background

Data protection is an important legal compliance issue for Amatis Training Ltd. During the course of the organisation's activities it collects, stores and processes personal data (sometimes sensitive in nature) about employees, delegates, suppliers and other third parties. It is therefore an area where all staff have a part to play in ensuring we comply with and are mindful of our legal obligations, whether that personal data is sensitive or routine.

The Data Protection Act 1998 was changed on 25 May 2018 with the implementation of the General Data Protection Regulation (**GDPR**). This is an EU Regulation that is directly effective in the UK and throughout the rest of Europe. A new Data Protection Act 2018 has also been passed to deal with certain issues left for national law. In particular, in the context of our safeguarding obligations, Amatis Training Ltd has a heightened duty to ensure that the personal data of candidates is at all times handled responsibly and securely.

While this new law does set out useful legal grounds in this area, in most ways this new law is strengthening the rights of individuals and placing tougher compliance obligations on organisations that handle personal information. The Information Commissioner's Office (**ICO**) is responsible for enforcing data protection law and has powers to take action for breaches of the law.

**Those who are involved in the processing of personal data are obliged to comply with this policy when doing so.** Accidental breaches will happen and may not be a disciplinary issue, but any breach of this policy may result in disciplinary action. [This policy may be amended at any time.]

This policy sets out the organisation's expectations and procedures with respect to processing any personal data we collect from data subjects.

Key data protection terms used in this data protection policy are:

- **data controller** – an organisation that determines the purpose and means of the processing of personal data. For example, the organisation is the controller of candidates' personal information. As a data controller, we are responsible for safeguarding the use of personal data;
- **data processor** – an organisation that processes personal data on behalf of a data controller, for example a payroll provider or other supplier of services;
- **personal data breach** – a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data;
- **personal information (or personal data)**: any information relating to a living individual (a data subject), including name, identification number, location or online identifier such as an email address. Note that personal information created in the ordinary course of work duties (such as in emails, notes of calls, and minutes of meetings) is still personal data and regulated by data protection laws, including the GDPR. Note also that it includes expressions of opinion about the individual or any indication of someone's intentions towards that individual;
- **processing** – virtually anything done with personal information, including obtaining or collecting it, structuring it, analysing it, storing it, sharing it internally or with third parties (including making it available to be viewed electronically or otherwise), altering it or deleting it;
- **special categories of personal data** – data relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health and medical conditions, sex life or sexual



orientation, genetic or biometric data used to identify an individual. There are also separate rules for the processing of personal data relating to criminal convictions and offences.

### Data Protection Lead

Amatis Training Ltd has appointed the Director as the Data Protection Lead who will endeavour to ensure that all personal data is processed in compliance with this Policy and the principles of the GDPR. Any questions about the operation of this policy or any concerns that the policy has not been followed should be referred in the first instance to the Data Protection Lead [dpl@amatistraining.com](mailto:dpl@amatistraining.com).

### The Principles

The GDPR sets out six principles relating to the processing of personal data which must be adhered to by data controllers (and data processors). These require that personal data must be:

1. processed **lawfully, fairly** and in a **transparent** manner;
2. collected for **specific and explicit purposes** and only for the purposes it was collected for;
3. **relevant** and **limited** to what is necessary for the purposes it is processed;
4. **accurate** and kept **up to date**;
5. **kept for no longer than is necessary** for the purposes for which it is processed; and
6. processed in a manner that ensures **appropriate security** of the personal data.

The GDPR's 'accountability' principle also requires that the Amatis Training Ltd not only processes personal data in a fair and legal manner but that we are also able to *demonstrate* that our processing is lawful.

This involves, among other things:

- keeping records of our data processing activities, including by way of logs and policies;
- documenting significant decisions and assessments about how we use personal data; and
- generally having an 'audit trail' vis-à-vis data protection and privacy matters, including for example when and how our Privacy Policy(s) are updated, how and when data protection consents were collected from individuals, how breaches were dealt with, etc.

### Lawful grounds for data processing

Under the GDPR there are several different lawful grounds for processing personal data. One of these is consent. However, because the definition of what constitutes consent has been tightened under GDPR (and the fact that it can be withdrawn by the data subject) it is generally considered preferable to rely on another lawful ground where possible.

One of these alternative grounds is 'legitimate interests', which is the most flexible basis for processing. However, it does require transparency and a balancing assessment between the rights of the individual and the interests of the Controller. It can be challenged by data subjects and also means the Controller is taking on extra responsibility for considering and protecting people's rights and interests. The organisation's legitimate interests are set out in its Privacy Policy, as GDPR requires.

Other lawful grounds include:

- compliance with a legal obligation, including in connection with employment and diversity;
- contractual necessity, e.g. to perform a contract with employees;



- a narrower set of grounds for processing special categories of personal data (such as health information), which includes explicit consent, emergencies, and specific public interest grounds.

## Headline responsibilities of all employees

### Record-keeping

It is important that personal data held by Amatis Training Ltd is accurate, fair and adequate. You are required to inform the organisation if you believe that *your* personal data is inaccurate or untrue or if you are dissatisfied with the information in any way. Similarly, it is vital that the way you recording the personal data of others – in particular colleagues, candidates and suppliers – is accurate, professional and appropriate.

Staff should be aware of the rights set out below, whereby any individuals about whom they record information in emails and notes on Amatis Training Ltd business may have the right to see that information. This absolutely must not discourage employees from recording necessary and sometimes difficult records of incidents or conversations involving colleagues or candidates, in accordance with the organisation's other policies, and grounds may sometimes exist to withhold these from such requests. However, the starting position is to record every document or email in such a way that you would be able to stand by it if the person about whom it was recorded were to see it.

### Data handling

All employees have a responsibility to handle the personal data which they come into contact with fairly, lawfully, responsibly and securely and in accordance with the employee handbook and all relevant policies and procedures. In particular, there are data protection implications across a number of areas of the organisation's wider responsibilities such as safeguarding and IT security, so all employees should read and comply with the following policies:

- ICT Acceptable Use policy
- Staff Code of Conduct
- Safeguarding

Responsible processing also extends to the creation and generation of new personal data / records, as above, which should always be done fairly, lawfully, responsibly and securely.

### Avoiding, mitigating and reporting data breaches

One of the key new obligations contained in the GDPR is on reporting personal data breaches. Data controllers must report certain types of personal data breach (those which risk an impact to individuals) to the ICO within 72 hours.

In addition, data controllers must notify individuals affected if the breach is likely to result in a "high risk" to their rights and freedoms. In any event, Amatis Training Ltd must keep a record of any personal data breaches, regardless of whether we need to notify the ICO. If you become aware of a personal data breach you must notify [dpl@amatistraining.com](mailto:dpl@amatistraining.com). If employees are in any doubt as to whether you should report something, it is always best to do so. A personal data breach may be serious, or it may be minor, and it may involve fault or not, but the organisation always needs to know about them to make a decision.



As stated above, Amatis Training Ltd may not need to treat the incident itself as a disciplinary matter – but a failure to report could result in significant exposure for the organisation, and for those affected, and could be a serious disciplinary matter whether under this Policy or the staff member's contract.

### Care and data security

More generally, we require all Amatis Training Ltd staff to remain conscious of the data protection principles (see section 3 above), to attend any training we require them to, and to use their best efforts to comply with those principles whenever they process personal information. Data security is not simply an online or digital issue but one that effects daily processes: filing and sending correspondence, notably hard copy documents. Employees should always consider what they most assured and secure means of delivery is, and what the consequences would be of loss or unauthorised access.

We expect all those with management / leadership responsibilities to be particular champions of these principles and to oversee the reporting of any concerns about how personal information is used by Amatis Training Ltd to [dpl@amatistraining.com](mailto:dpl@amatistraining.com), and to identify the need for (and implement) regular staff training.

### Rights of Individuals

In addition to the organisation's responsibilities when processing personal data, individuals have certain specific rights, perhaps most significantly that of access to their personal data held by a data controller (i.e. Amatis Training Ltd). This is known as the 'subject access right' (or the right to make 'subject access requests'). Such a request must be dealt with promptly (30 days) and does not need any formality, nor to refer to the correct legislation. If you become aware of a subject access request (or indeed any communication from an individual about their personal data), you must tell [dpl@amatistraining.com](mailto:dpl@amatistraining.com) as soon as possible.

Individuals also have legal rights to:

- require us to correct the personal data we hold about them if it is inaccurate;
- request that we erase their personal data (in certain circumstances);
- request that we restrict our data processing activities (in certain circumstances);
- receive from us the personal data we hold about them for the purpose of transmitting it in a commonly used format to another data controller;
- object, on grounds relating to their particular situation, to any of our particular processing activities where the individual feels this has a disproportionate impact on them; and
- object to automated individual decision-making, including profiling (where a significant decision is made about the individual without human intervention), and to direct marketing, or to withdraw their consent where we are relying on it for processing their personal data.

Except for the final bullet point, none of these rights for individuals are unqualified and exceptions may well apply. In any event, however, if you receive a request from an individual who is purporting to exercise one or more of their data protection rights, you must tell [dpl@amatistraining.com](mailto:dpl@amatistraining.com) as soon as possible.

### Data Security: online and digital

Amatis Training Ltd must ensure that appropriate security measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data. As such, no member of staff is permitted to remove personal data from organisation's premises,



whether in paper or electronic form and wherever stored, without prior consent of the Director. Where a worker is permitted to take data offsite it will need to be encrypted.

### Processing of Credit Card Data

Amatis Training Ltd complies with the requirements of the PCI Data Security Standard (PCI DSS). Staff who are required to process credit card data must ensure that they are aware of and comply with the most up to date PCI DSS requirements. If you are unsure in this regard, please seek further guidance from the Data Protection Lead.

### Summary

“It is in everyone's interests to get data protection right and to think carefully about data protection issues: this means handling all personal information with which you come into contact fairly, lawfully, securely and responsibly.

A good rule of thumb here is to ask yourself questions such as:

- Would I be happy if my own personal information were being used (for example, shared with a third party) in the way I am proposing? Would I expect it?
- Would I wish to stand by how I have recorded this information in an email or official record if the person concerned was able to see it?
- What would be the consequences of my losing or misdirecting this personal data?

Data protection law is therefore best seen not as oppressive red tape, or a reason not to do something necessary or important, but a code of useful and sensible checks and balances to improve how handle and record personal information and manage our relationships with people. This is an important part of the organisation's culture and all its staff and representatives need to be mindful of it.”