# GDPR Compliance Procedures

How we handle rights requests, data breaches, records of processing, data protection by design and suppliers.

| | |
|---|---|
| **Document** | GDPR Compliance Procedures |
| **Organisation** | NC Safety Solutions |
| **Document owner** | Nedim Custic, DipNEBOSH, CEO |
| **Version** | 1.1 |
| **Effective date** | 12th September 2026 |
| **Next review** | 12th September 2027, or sooner if the law, our services or our organisation change |
| **Revision history** | 1.0, 9th September 2026: first issue. 1.1, 12th September 2026: reissued under the NC Safety Solutions name, with the insurance statement updated. |

## 1. Purpose

These procedures set out how NC Safety Solutions puts its Data Protection Policy into practice day to day: how we handle rights requests, personal data breaches, records of processing, data protection by design, and suppliers. They apply to everyone who works with or for us.

## 2. Rights requests (subject access and others)

Requests can be made informally by emailing **nedim@ncsafetysolutions.co.uk**. No form is required, and a request made to any of our people, by any channel, must be passed to the CEO on the day it is received.

1. **Log the request** with the date received, the requester, the right being exercised and any deadline.
2. **Confirm identity** before releasing any data, using reasonable means proportionate to the sensitivity of the data.
3. **Clarify the scope** with the requester if the request is very broad, without pausing the clock unless the clarification is genuinely needed.
4. **Search** all relevant systems, including email, document storage and any paper records.
5. **Review** the material for third-party data and exemptions, and redact where lawful and necessary.
6. **Respond** within one calendar month of receipt. If a request is complex or numerous, we may extend by up to two further months and will tell the requester within the first month.
7. **Record** the outcome and the date of response in the log.

This covers all UK GDPR rights: access, rectification, erasure, restriction, portability and objection. Requests are free of charge unless manifestly unfounded or excessive, in which case we may charge a reasonable fee or refuse and explain why.

## 3. Personal data breaches

A personal data breach is a security incident that leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. Examples include a lost laptop, an email sent to the wrong recipient, or unauthorised access to an account.

8. **Report** any suspected breach to the CEO immediately upon discovery.
9. **Contain** the breach, for example by recalling an email, changing passwords or remotely wiping a device.
10. **Assess** the risk to people's rights and freedoms, considering the type and volume of data, who is affected and what harm could follow.
11. **Notify the ICO** within 72 hours of becoming aware where the breach is likely to result in a risk to individuals. Where the risk is high, also inform the affected people without undue delay, telling them what happened and what they can do.
12. **Notify clients** without undue delay where we are acting as their processor.
13. **Record** every breach, notifiable or not, in the breach log with its causes, the assessment, and the action taken to prevent recurrence.

## 4. Records of processing

We keep a record of the personal data we process. For each processing activity the record states:

| Field | Content |
|---|---|
| Activity | What we do, for example "responding to enquiries" or "client accident record review". |
| Data categories and subjects | What data is involved and whose it is. |
| Purpose and lawful basis | Why we process it and the UK GDPR basis, plus the Article 9 condition for special category data. |
| Storage and location | Where it is held and whether any transfer outside the UK takes place. |
| Recipients | Who it is shared with, including processors. |
| Retention | How long we keep it and what happens at the end. |
| Security measures | The main technical and organisational controls applied. |

The record is reviewed alongside the Data Protection Policy and updated whenever a new activity, tool or supplier is introduced.

## 5. Data protection by design

Before taking on a new tool, supplier or type of processing, we consider the data protection impact first: whether the data is needed at all, where it will be stored, who can access it, and what could go wrong. We choose the least intrusive option that meets the need.

Higher-risk processing, for example large-scale processing of health data or the use of new monitoring technology, receives a documented Data Protection Impact Assessment (DPIA) before it starts. Where a DPIA identifies a high risk that cannot be reduced, we consult the ICO before proceeding.

## 6. Suppliers and processors

Suppliers that process personal data for us, such as hosting and email providers, are used only under contracts containing the processor obligations required by Article 28 UK GDPR. Before appointing a supplier we check that it offers appropriate security measures and, where relevant, appropriate international transfer safeguards. We keep a list of current processors in the record of processing and review it annually.

## 7. Privacy information

We give individuals the information required by Articles 13 and 14 UK GDPR through our Privacy Notice, which is published on our website and referenced in proposals and engagement documents. Where we collect personal data for a new purpose, we update the notice first.

## 8. Marketing

We send marketing only to business contacts where we have a legitimate interest or consent, in line with the Privacy and Electronic Communications Regulations. Every message includes a simple way to opt out, and opt-outs are actioned immediately and recorded.

## 9. Training and awareness

Everyone who works with or for us is briefed on these procedures when they join and whenever the procedures change. The CEO maintains their own knowledge of data protection law as part of continuing professional development.

## 10. Complaints

Anyone unhappy with how we handle their data can contact us at **nedim@ncsafetysolutions.co.uk**, and has the right to complain to the Information Commissioner's Office at ico.org.uk. Complaints about data handling are also recorded under our Complaints Procedure.

## 11. Review

These procedures are reviewed at least annually, after any notifiable breach, and whenever the Data Protection Policy changes.

Approved and issued by

**Nedim Custic, DipNEBOSH - CEO**
NC Safety Solutions
12th September 2026