

Data Protection Policy



Policy Scope: This policy relates to all employees, subcontractors, consultants and partners. This policy details user responsibilities and arrangements for the control of personal and business information in line with the General Data Protection Regulations (GDPR) enacted by the Data Protection Act 2018.

Novus Property Solutions Ltd. (the Company) comply with the requirements of the General Data Protection Regulation (GDPR) by following procedures to ensure that all data users who have access to any personal data held by or on behalf of the Company are fully aware of and abide by their duties under the GDPR.

To perform our business, Novus needs to collect, store and use information about 'people'. 'People' include members of the public, current, past and prospective employees, customers and suppliers, collectively referred to as data subjects. This personal data will be handled according to the GDPR irrespective of how it is collected, recorded and used and whether present on paper, in computer records or recorded by other means.

At Novus, we regard the lawful and appropriate treatment of personal information as important to our successful operations, reputation and as essential to maintaining confidence between us and those with whom we carry out business. We therefore fully endorse and comply with the Principles of the GDPR.

Handling Personal Data

Through management and use of appropriate controls, Novus and our employees commit to:

- ✦ Using personal data in the most efficient way.
- ✦ Collecting and processing the data or information which is needed and no more.
- ✦ Using personal data as described on collection, or for purposes which are legally permitted.
- ✦ Ensuring personal data is accurate and remains current.
- ✦ A data retention schedule will be maintained for data that is processed regularly, and we will ensure personal data is retained for no longer than is necessary.
- ✦ Securely destroying personal data which is no longer needed.
- ✦ Adopting appropriate technical and organisational measures to safeguard personal data.
- ✦ Ensuring that personal data is not transferred outside the EEA without suitable safeguards.
- ✦ Making information available to data subjects of their rights to access personal data.
- ✦ Ensuring that the following rights of data subjects can be fully exercised:
 - to be informed
 - to provide access to personal information
 - to request rectification
 - to request erasure
 - to restrict processing in certain circumstances
 - to data portability
 - to object to processing

Data Protection Principles

Processing of personal data will comply with seven principles of good practice. Personal data shall be:

- ✦ Processed lawfully, fairly and in a transparent manner.
- ✦ Collected for specified, explicit and legitimate business purposes and not further processed or stored in a manner that is incompatible with those purposes.
- ✦ Limited at point of collection to what is necessary for the specified business purpose.
- ✦ Accurate and up to date, with reasonable steps taken to erase personal data that is inaccurate.

- ◆ Kept for no longer than is necessary and only for the stated business purposes.
- ◆ Kept private, with protection against unauthorised processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.
- ◆ Comply with robust data protection policies, regular audits, staff training, and all processing activities fully documented.

Sensitive Personal Data

The Company holds limited amounts of Sensitive Personal Data which has been identified and will be subject to the special processing stipulated by the GDPR. Where significant volumes of new data, or where new sensitive data or heightened risk is generated from data collection, a Data Protection Impact Assessment (DPIA) will be completed by the Data Protection Officer or Deputy Data Protection Officer.

The characteristics which classify a piece of data sensitive are:

- ◆ Racial or ethnic origin
- ◆ Political opinion
- ◆ Religious/philosophical beliefs
- ◆ Trade union membership
- ◆ Physical or mental health or condition
- ◆ Sexual life or sexual orientation
- ◆ Biometric data

Handling Personal Data of Minors

In accordance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018, the organisation recognises the heightened need for safeguarding the personal data of individuals under the age of 18.

- ◆ **Lawful Basis and Consent:** Personal data relating to minors will only be collected and processed where a clear lawful basis exists. Where consent is required, it must be obtained from a person with parental responsibility unless the minor is deemed competent to provide their own consent under applicable UK law.
- ◆ **Data Minimisation and Purpose Limitation:** Only data strictly necessary for the intended purpose will be collected. The organisation will not use minors' data for profiling, marketing, or automated decision-making unless explicitly justified and legally permitted.
- ◆ **Security and Access Controls:** Personal data of minors will be subject to robust security measures. Access will be restricted to authorised personnel only.
- ◆ **Retention and Deletion:** Data relating to minors will be retained only for as long as necessary to fulfil the purpose for which it was collected, after which it will be securely deleted in accordance with the organisation's retention schedule.
- ◆ **Special Considerations:** Where minors are engaged through apprenticeships, outreach programmes, or community initiatives, additional safeguards will be applied, including Data Protection Impact Assessments (DPIAs) where appropriate.

Responsibilities

All staff are responsible for ensuring that the minimum standards established within this policy are adhered to in line with their specific role and responsibilities. Heads of Departments and Heads of Operations are responsible for ensuring their departments are compliant with GDPR requirements and where this is not possible or is unknown, to flag this risk to their Executive Director and the Data Protection Officer.

Novus require all users to complete regular Information Security courses, designed to educate and raise awareness about the importance of employing good information security practice in day-to-day tasks to facilitate and promote appropriate use and safety of information assets. The courses are mandatory for all colleagues and users with completion of the courses monitored and reported by the IT department.

The Company Board devolves responsibility for policy execution to the Departmental Managers, Head of Operations and Operations Managers who must apply the Data Protection procedures. The Data Protection Officer (DPO) will assist these managers in procedure application and business process revision that involves personal data. The DPO will periodically monitor policy compliance through internal audit.

Data Sharing

Data sharing with our supply chain and contractors is a critical part of service delivery. However, the responsibility for ensuring data remains secure and processed correctly remains with Novus when we transfer data to a third party. When sharing data, you must follow the key principles in data protection legislation:

- ✦ The accountability principle means that you are responsible for your compliance, and you must be able to demonstrate that compliance through appropriate records of what data is shared, what checks have been carried out.
- ✦ You must share personal data fairly and transparently & You must identify at least one lawful basis for sharing data before you start any sharing. This includes ensuring personal data is processed based on one or more of the following grounds:
 - Consent – you have permission to process the data.
 - Contractual necessity.
 - Legal obligation.
 - Vital interests.
 - Public task.
 - Legitimate interest.
- ✦ You must process personal data securely, with appropriate organisational and technical measures in place.
- ✦ It is your responsibility to satisfy yourself about the integrity of the data supplied to you.

When you share data with a third party, there must be a contract in place with the relevant GDPR clauses, and it is good practice to have a data sharing agreement in place as well. Appendix C contains a data sharing checklist for you to use when transferring data to subcontractors and supply chain partners. If you need further support, please contact the Novus Data Protection Officer.

Data Breach

A personal data breach is “a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data, whether by accidental or deliberate causes”. The General Data Protection Regulation (GDPR) introduces a duty on all organisations to report certain types of personal data breach to the relevant authority.

Data breaches must be reported and managed in a timely manner and reported as soon as a breach or potential breach is discovered. The DPO or the Head of IT & Data will align the management response to a data breach with the Crisis Management Policy.

A data breach can include the following:

- ◆ Access to personal data by an unauthorised third party.
- ◆ Deliberate or accidental action (or inaction) by a controller or processor.
- ◆ Sending personal data to an incorrect recipient.
- ◆ Hand-held devices / laptops containing personal data being lost or stolen.
- ◆ Alteration of personal data without permission; and
- ◆ Loss of availability of personal data.

Practical examples of breaches I should report to the Data Protection Officer (DPO):

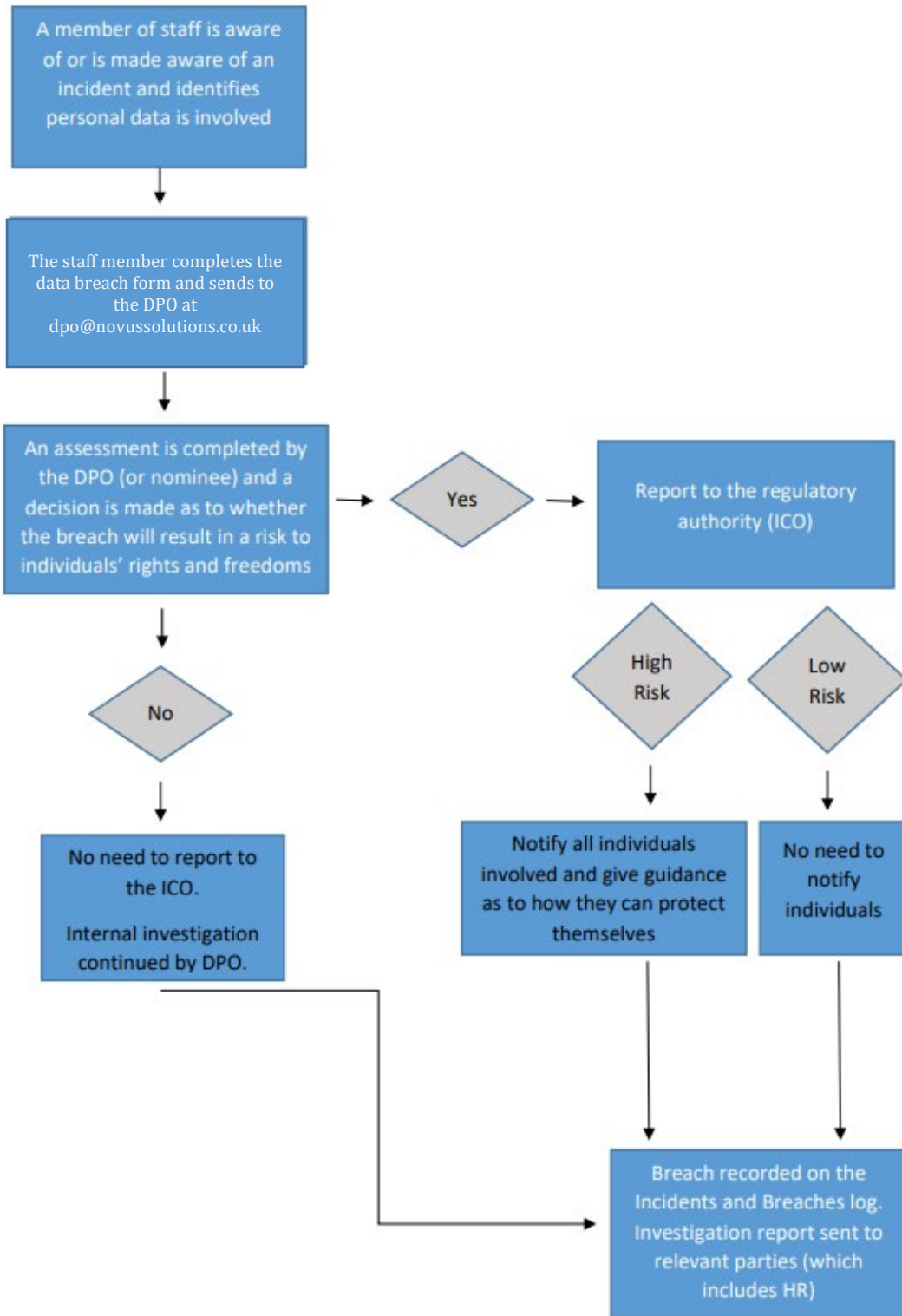
- ◆ My work laptop has been stolen (from work or elsewhere).
- ◆ I sent a letter or file to a customer but sent the wrong letter or file to the wrong customer.
- ◆ I sent a document containing sensitive information to the wrong colleague.
- ◆ I sent a customer address list to a subcontractor without having the correct contractual clauses in place.
- ◆ A subcontractor uses a third party to carry out works on Novus's behalf and doesn't complete the necessary "Third Party" paperwork and checks.

Data Subject Access Request

In accordance with Article 15 of the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018, Novus Property Solutions Ltd recognises the right of individuals to access their personal data. This clause outlines the process for handling DSARs within the organisation. Appendix D sets out the DSAR process.

Appendix A

Data Breach workflow



Appendix B

DATA BREACH - REPORTING FORM

In the box below, please describe in as much detail as you can, the nature of the personal data breach:

Please fill in the following details:

Your Name:	
Your Department:	
Date of Breach:	
Date of Reporting:	
Approximate number of individuals data concerned:	
Is there any sensitive personal data involved: If YES – please give full details	
Are there any subjects under the age of 18 If YES – approx. how many?	
Have you taken any action to rectify the issue at the time of reporting? If so what action?	

Please email a completed copy of this form to the Data Protection Officer: dpo@novussolutions.co.uk

Appendix C

Data Sharing Checklist

- Is any of it special category data (or does it involve sensitive processing under Part 3 of the DPA 2018)?
- What additional safeguards will you have in place?
- How should you share the information?
 - You must share information securely.
 - You must ensure you are giving the information to the right recipient.
- What is to happen to the data at every stage?
- Who in each organisation can access the shared data? Ensure it is restricted to authorised personnel in each organisation.
- What organisation(s) will be involved? You all need to be clear about your respective roles.
- How will you comply with your transparency obligations?
 - Consider what you need to tell people about sharing their data and how you will communicate that information in a way that is concise, transparent, easily accessible and uses clear and plain language.
 - Consider whether you have obtained the personal data from a source other than the individual.
 - Decide what arrangements need to be in place to comply with individuals' information rights. Bear in mind the differences under Part 3 of the DPA 2018, if applicable.
- What quality checks are appropriate to ensure the shared data is accurate and up to date?
- What technical and organisational measures are appropriate to ensure the security of the data?
- What common retention periods for data do you all agree to?
- What processes do you need to ensure secure deletion takes place?
- When should regularly scheduled reviews of the data sharing arrangement take place?

Appendix D – Data Subject Access Request Procedure

Data Subject Access Request (DSAR) Process

In accordance with Article 15 of the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018, Novus Property Solutions Ltd recognises the right of individuals to access their personal data. This clause outlines the process for handling DSARs within the organisation.

1. Submitting a Request

Individuals may submit a DSAR by contacting the Data Protection Officer (DPO) via email at dpo@novussolutions.co.uk or by post to HR Department Five Towns House, Hillside, Festival Way, Stoke-on-Trent, ST1 5SH. Requests must include sufficient information to verify the identity of the requester and locate the data in question.

2. Acknowledgement and Timeline

Upon receipt of a DSAR, the DPO will acknowledge the request within five working days. The organisation will respond to the request within one calendar month, starting from the day the request is received. If the request is complex or involves a large volume of data, the response period may be extended by a further two months, with notification to the requester.

3. Verification and Scope

The DPO will verify the identity of the requester and assess the scope of the request. If additional information is required to confirm identity or clarify the request, the response timeline will pause until the necessary details are received.

4. Data Retrieval and Review

Relevant departments will be instructed to retrieve all personal data relating to the requester. The DPO will review the data to ensure that:

- It does not include third-party personal data without consent.
- It does not compromise commercial confidentiality or security.
- It complies with legal exemptions under the Data Protection Act 2018.

5. Response Format

The response will include:

- A copy of the personal data.
- The purposes of processing.
- The categories of personal data concerned.
- The recipients or categories of recipients to whom the data has been disclosed.
- The retention period or criteria used to determine it.
- Information about the individual's rights under UK GDPR.

6. Refusals and Exemptions

If the organisation refuses to comply with a DSAR, the requester will be informed of the reasons and their right to complain to the Information Commissioner's Office (ICO). Grounds for refusal may include manifestly unfounded or excessive requests, or legal exemptions.

7. Record Keeping

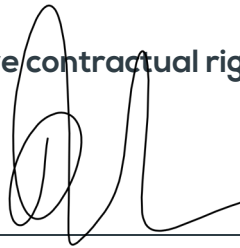
All DSARs will be logged and retained for audit purposes. The log will include the date received, response date, nature of the request, and outcome.

8. Complaints and Escalation

If a requester is dissatisfied with the response, they may escalate the matter to the DPO or lodge a complaint with the ICO.

This policy does not give contractual rights to individual colleagues.

Authorised by:



Executive Director

Document History:

Version	Issue Date	Review Date	Author	Comments
0	31 st July 2019	31 st July 2020	Neil Washington	New policy following company review
A	20 th Nov 2019	20 th Nov 2020	Alan Nixon	This policy does not give contractual rights to individual colleagues. Added.
A	20 th Nov 2020	20 th May 2021	Alan Nixon	No changes. Short review date due to restructuring.
B	May 2021	May 2022	David Leach	New policy format New policy number
C	May 2022	May 2023	David Leach	Data breach process added
D	July 2023	July 2024	David Leach	Data Sharing section added and Data Sharing Checklist added
E	July 2024	July 2025	David Leach	Added reference to Crissi Management Policy. Updated Practical Examples of Data Breach. HOO's & HOD's responsibilities and removed reference to USB devices.
F	August 2025	August 2026	David Leach	Added reference to DPIA, DSAR and processing of data from those aged under 18.