Graham Holmes Astraseal Ltd

DATA PROTECTION POLICY

The 'Company' herein comprises:-

Graham Holmes Astraseal Ltd [Company Registered in England, Number 2593809

The Company is at various times a data controller and/or a data processor.

General Statement of the Company's Duties and Scope of this Policy

The Company is required to process relevant personal data relating to:-

1. The Company's Employees,
2. The Company's Subcontractors/their Employees
3. Staff/Labour supplied by Agencies, and
4. Proprietors/Employees of our Suppliers and Customers

as part of its operations, and shall take all reasonable steps to do so in accordance with this Policy.

The Company recognises the rights of all individuals with whom it comes into contact - both internally and externally - and is committed to full compliance with the General Data Protection Regulation (GDPR).

Definitions

In this Policy the following terms have the meaning(s) stated:-

'Data Subject' means (a) person(s) who can be identified through Data.

'Data' means information - which may include facts and opinions - from which any individual(s) can be identified: for example, information necessary for employment such as name and address, details for payment of salary/wages/fees (including UTR/NI Numbers), bank account details and attendance/ timekeeping records. It may also include, personal e-mail addresses/phone numbers/IP addresses, etc.

We will only know the full extent of GDPR's reach in the UK once it is established through case law; but at this point the Company does not anticipate that people's work phone numbers/business e-mail addresses/IP Addresses of company-owned computers/phones will constitute 'Data'.

'Special Category Data' (Sensitive Data) includes information relating to medical matters, Disability, Age, Race, Religion or Belief, Sexual Orientation, Gender, Gender Reassignment, Marriage/Civil Partnership, Pregnancy/ Maternity, Political Opinions/Affiliations, Trade Union membership, etc.

'Parental Consent' means the prior express consent of a Parent or Guardian in respect of a person under 13 years of age.

'Explicit Consent' requires a very clear and specific consent action/statement of consent. It will not be sufficient to invite the ticking of a box when a Data Subject does not want their data to be processed. GDPR requires consent to be a "freely given, specific, informed and unambiguous indication of the Data Subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.".

Persons Responsible for the Implementation and Operation of this Policy

The Company is not required to appoint a Data Protection Officer under GDPR because:-

i. the Company is not a public authority;
ii. its core activities do not require large scale, regular and systematic monitoring of individuals; and
iii. its core activities do not consist of large scale processing of special categories of data or data relating to criminal convictions and offences.

However, the Company has appointed persons to act as Data Contacts and to be the 'first port of call' for all data protection-related enquiries, Subject Access Requests and communication of routine concerns.

Colin Stanley (Operations Director)

Astraseal House, Paterson Road, Finedon Road Industrial Estate, Wellingborough, Northants NN8 4EX

Tel: 01933 227233. E-mail: colinstanley@astraseal.com

Principles

The Company will take all reasonable steps to ensure that all Data is:-

Fairly and lawfully processed
Processed for a lawful purpose
Adequate, relevant and no more than is necessary
Accurate and up-to-date
Not kept for longer than is necessary
Processed in accordance with the Data Subject's rights and with GDPR
Secure

Only transferred to any other country (e.g. in the 'cloud' hosted by Microsoft within the EU) with adequate protection.

The Company is an equal opportunities employer and never intentionally requests, stores or processes information about anyone's Race, Religion or Belief, Sexual Orientation, Gender, Gender Reassignment, Political Opinion/Affiliation or Marriage/Civil Partnership.

The Company will obtain/store/process/forward the minimum information necessary to comply with its legal obligations (including but not limited to Health & Safety), to carry out its obligations under a contract of employment, service, etc. and in order to pursue its Legitimate Interests/trade effectively in regard to:-

Disability (e.g. so as to make all reasonable adjustments to accommodate an individual and/or for Insurance purposes),

Pregnancy/Maternity (in order to agree suitable arrangements, arrange maternity leave cover, etc.),

Age (e.g. for Insurance purposes and/or to ensure that an individual is not statute-barred from a particular activity such as under-age driving or carrying out certain controlled activities on site without adult supervision, etc.),

and will securely dispose of it at the earliest reasonably practical opportunity (albeit that statute and/or the Company's Legitimate Interests may necessitate the retention of such Data for a considerable length of time).

Certain motoring offences (including causing death by dangerous/careless driving, dangerous driving and driving whilst under the influence of drink or drugs) are Criminal Offences. In the case of employees/ subcontractors/agency labour who drive motor vehicles in connection with the Company's business the Company is obliged to obtain and process this Data and to pass it on to others and to store it for as long as is necessary, in order to obtain Insurance quotations and to comply with the conditions of Insurance cover and/or to defend any civil claim or prosecution (e.g. Corporate Manslaughter, etc.). Until such time as the Data Protection Bill is enacted/comes into force, the Company will rely on HM Government's Statement Of Intent on Data Protection dated 07.08.17 which sets out unequivocally the Government's intention to pass UK legislation to continue to allow all organisations to process Criminal Conviction data for Insurance purposes. Otherwise, the Company will continue to comply with the Rehabilitation Of Offenders Act 1974 and the Rehabilitation Of Offenders Act 1974 (Exceptions) Order 1975.

The Company will not obtain/process/store information on any person under 16 years of age. In the case of persons aged 16 or 17 years of age, although Parental Consent is not required under GDPR, particular care will be taken when obtaining/relying on consent to ensure that such consent is fully informed and freely given.

The Company will obtain/store/process/forward the minimum details of medical history and current medical conditions necessary and only retain such Data for as long as is reasonably required (albeit that

statute and/or the Company's Legitimate Interests may necessitate the keeping of such Data for a considerable length of time).

Data Protection Impact Assessment (DPIA)

The Directors carried out a DPIA covering all aspects of the Company's activities, processes and systems during March and April 2018.

Wherever 'Data' was found to be *at risk*, the Directors considered the proportionality of the importance of the Data gathering/processing/passing to third parties against the risk to Data Subjects, then implemented measures to mitigate such risk.

The Directors considered whether the collecting/processing of any of the *at risk* Data could be stopped/ reduced, but the reality is that the Company trades within a highly regulated, Health & Safety-orientated industry where there is inherent danger and a very high propensity for personal injury claims whether real or 'trumped-up', and where commercial disputes are the norm (with some leading to litigation).

The Company is subject to complex and demanding statutes requiring insurance, training, qualifications, monitoring of health & fitness for the task(s) in hand, etc.: all of which involves the gathering and processing of personal Data - some of which is Special Category/Sensitive Data - and the passing of it to third parties. We must also have access to/the use of vehicle tracking records and records of attendance at Site in order to investigate - and if appropriate, to counter - allegations by Main Contractors of short hours worked by Graham Holmes Astraseal Ltd`s Operatives and to defend the Company and its officials in any prosecution (e.g. for Corporate Manslaughter/ negligence/alleged offences under the Working Time Regulations).

Having put in place measures to mitigate those risks the Directors took the view that the Company's legal obligations, Legitimate Interests, contractual obligations, etc. outweigh the risks to Data Subjects.

Processing of Data

Following the DPIA and HR Audit, a training programme is underway.

Management and Operatives have been/are being informed by memo, in meetings and in group/one-to-one training of the importance of Data Protection and the severe penalties which will be levied against businesses which fail to comply with GDPR and/or permit a Data Breach. Employees have been/are being instructed as to what constitutes a Data Breach or a Serious Data Breach and to report it to a Director within one working hour of discovery; so that the Company can report it within 72 hours to the data protection authorities if required. Although circumstances and evidence will be taken into consideration, the 'default' penalty for any failure to report a Data Breach or a Serious Data Breach to a Director within the specified time period is summary dismissal for Gross Misconduct.

The Company's Rules and Disciplinary Procedure have been amended and the Employee Handbook updated to reflect our Zero Tolerance of misuse of the Company's IT equipment/systems and phones. Employees are being informed that although circumstances and evidence will be taken into consideration, the 'default' penalty for any such offence is summary dismissal for Gross Misconduct.

Under GDPR, Consent is not required for Data to be obtained/processed/stored/transmitted to third parties provided that there is a valid Legal Basis, and a necessity to do so. Such necessities and Legal Bases are set out in the Company's Privacy Notices and include but are not limited to the obtaining/ processing/storage/passing on of Data which is necessary for:

i. the performance of a contract of employment/service (e.g. Names & Addresses, UTR/NI Numbers, P45/P46 Forms, wage/salary records, CSCS Cards/NVQ records, Bank Account details, etc.),
ii. compliance with Legal obligations (i.e. statutes/statutory instruments, etc), and
iii. the Company's Legitimate Interests (e.g. to bring/defend actions in the Courts/Arbitrations/ Adjudications/Tribunals, defend prosecutions, for the prevention/detection of fraud, etc.).

Data will be kept confidential and secure. It will only be passed to third parties where necessary; which includes but is not limited to circumstances in which there is a Legal Obligation, where the Company is obliged to provide Qualifications and/or proof of right to work in the UK and/or proof of attendance at Site/work carried out to the Company's clients, or where the Company is seeking advice etc. from its legal/professional advisors/consultants or in preparation for/in the course of bringing/defending actions in the Courts/Arbitrations/Adjudications/Tribunals, etc.

The Company requires all third parties to demonstrate that they observe similar standards of care in accordance with GDPR. Third Parties processing Data as external processors (e.g. service providers, 'cloud' services, incl. storage, web sites, etc.) will be required to demonstrate compliance with this Policy and with GDPR. The Company's Supply Chain is being invited to provide evidence of their GDPR compliance or to give an irrevocable Warranty that they will fully abide by Graham Holmes Astraseal Ltd's Data Protection Policy, Data Security Policy, Privacy Notices and practices and will take full responsibility for any failure to do so.

Although we do not market to individuals, the Company will exercise particular care in its sales/ marketing strategy; seeking Explicit Consent wherever it is needed. The Company recognises Data Subjects' absolute right to object to Direct Marketing. The Company's websites are being updated to include our Privacy Notice and to give greater choice to visitors as to how their Data may and may not be used.

The Company will never sell or give away its Customer/Supplier Lists.

The Company will exercise particular care in processing Special Category Data/Data concerning Criminal Convictions. Only the Company's Directors and authorised Data Contact will process such Data; save for where a Contracts Manager is obliged to forward to the Company's client the name and special requirements, if any, of a disabled or less able worker. The Legal Bases and relevant 'Article 9'/'Article 10' Conditions are set out in the Company's Privacy Notices.

Wherever consent is sought, Data Subjects will be invited to positively say that they DO consent to the obtaining/processing/storage/forwarding of Data; and without this, no consent will assumed/implied/ inferred.

Right Of Access/Data Subject Access Requests

Under GDPR, citizens have the right to request access all of their personal Data and to request rectification of anything that is inaccurate. There is also a right to object to processing/request restricted processing of Data and/or to ask that Data is completely erased and/or to request Data Portability; although the Company may resist such request(s) if there is justification to do so. Each request carries a timeframe and a deadline of one month (which can only be extended in mitigating circumstances), from the original date of request.

The grounds on which a request to erase may be refused include, but are not limited to such information as the Company may require in order to assist our Insurers and/or to defend a current/potential claim in the Courts (e.g. for personal injury, defects liability, etc.) or a current/ potential prosecution or a current/potential action in an Employment Tribunal/ Employment Appeals Tribunal.

These rights are clearly set out in the Company's Privacy Notices.

Supply Chain

As stated above, the Company expects its Suppliers, Subcontractors, Consultants, etc. to be GDPR-compliant. We are therefore currently undertaking 'GDPR due diligence' on our Supply Chain.

Privacy Notices

Under GDPR, the Company is required to describe to individuals what we are doing with their Data. Graham Holmes Astraseal Ltd.'s Privacy Notices set this out along with Data Subjects' rights.

Accuracy

The Company will use its best efforts to ensure that all Data held in relation to Data Subjects is accurate. Data subjects must notify the relevant Data Contact of any changes to information held about them (e.g. change of address).

Enforcement

If a Data Subject believes that the Company has not complied with this Policy or has acted otherwise than in accordance with GDPR they should utilise the Company's Grievance Procedure without delay (addressing their grievance to a Director) and make a report to the data protection authorities.

Data Security

The Company has taken/will take appropriate technical & organisational steps to ensure the security of Data. Details are more fully set out in the Company's Data Security Policy.
All Employees have been/are being made aware of their duties under GDPR. Employees are required to respect the Data and privacy of others and must ensure that appropriate protection and security measures are taken against the unlawful or unauthorised processing of Data and against the accidental loss of/damage to Data. Although circumstances and evidence will be taken into consideration, the default disciplinary sanction for inappropriate and/or unauthorised conduct in relation to Data is summary dismissal for Gross Misconduct.

An appropriate level of data security must be deployed for the type of Data and the particular data processing being performed. Data must be stored in appropriate systems or at the very least 'under lock and key' with restricted access to the keys. The use of encryption will be considered when Data is transported 'off site'.

Time Limits for Retention of Data

The Company trades within an exceptionally highly regulated and potentially hazardous industry, and the Company's Policy on Data Retention reflects this.

The Company will rely on Data in bringing or defending any Claim in a Court/Arbitration/Adjudication/ Tribunal or in defending any prosecution.

Tribunal Claims must normally be brought within three months but there is no time-limit on the bringing of Discrimination Claims, etc. The Limitation Act 1980, as amended, prescribes the time limit for commencement of contractual claims as six years from the cause of action and for the commencement of personal injury claims as three years from when the injury/condition first became apparent. The difficulty with the latter is that the symptoms associated with some conditions related to the kind of activities which the Company undertakes (e.g. HAVS) can take many years to appear. The Defects Liability period in most of the Company's contracts with its clients is twelve years; and worksheets/ wages records/qualifications may be needed on order to defend a Defects Liability Claim.

Hence, all Data pertaining to contracts of employment and the performance thereof, and Data pertaining to subcontracts and contracts of personal service will need to be held for a minimum of seven years. Data which could conceivably be required in a Defects Liability Claim - which in practical terms, means Data pertaining to any and all Site workers - must be retained for a minimum of twelve years. The Company will make reasonable efforts to securely destroy Data as soon as it can be safely concluded that it is no longer needed; but in the circumstances, the Company reserves its right to hold this data in perpetuity where necessary.

What follows is a non-exclusive list of examples of where Data will generally be retained for less than twelve years.

a. Recruitment. Data obtained from unsuccessful applicants will usually not be retained at all, and will be retained for no more than six months without the Explicit Consent of the Data Subject (other than were an Employment Tribunal Claim to have been brought or be mooted: in which case Data will be retained for the duration of the Claim up until a final determination is made by the Employment Appeals Tribunal or upon expiry of the period following the Tribunal's Judgment in which an Appeal can be commenced, whichever is the earlier).

b. Except as otherwise stated herein, Data obtained from successful applicants who's work does not materially affect Defects Liability (e.g. many office workers) will normally be retained for a minimum of seven years from Termination Of Employment in any event. Where any contractual claim is brought in a Court, Data will be retained for the duration of the Claim until a final determination is made by the Court Of Appeal or upon expiry of the period following the Court's Judgment in which an Appeal can be commenced, whichever is the earlier.

c. Payroll Records will be retained for seven years from Termination Of Employment in any event; and where any contractual claim is brought in a Court, Data will be retained for the duration of the Claim up until a final determination is made by the Court Of Appeal or upon expiry of the period following the Court's Judgment in which an Appeal can be commenced, whichever is the earlier.

d. References obtained from Employees' previous employers will be retained for as short a time as the Company considers appropriate; and for no more than two years in any event.

e. Records of disciplinary hearings and 'spent' disciplinary warnings will be retained for a minimum of seven years (for reasons stated above and because they may be needed to show a pattern of behavior), and for twelve years for site workers where they could reasonably be relevant to any current or future Defects Liability Claim.

f. Employees' Bank Account Details will be held no longer than is necessary (i.e. they will be securely destroyed following issue of Termination Pay & P45).

g. Copies of documents submitted as proof of right to work under the Asylum & Immigration Act 1996, as amended, will be retained for two years following termination of employment (for use in any potential investigation by the Immigration authorities). The Company recognises that copies of ID such as Passports may indicate a Data Subject's race, age, gender and/or gender reassignment; and that this is therefore Special Category Data. Nevertheless the Company's overriding duty is to uphold the law and to be seen to be doing so. Critically, such records must be retained for the specified period in respect of EVERY employee/agency worker regardless of race, age, gender, gender reassignment, etc. in order to prevent discrimination.

h. Medical Records will be retained for a minimum of seven years in order to defend any contractual claim. Medical records of Site Operatives will be retained for a minimum of seven years; or 40 years from the date of the last entry in relation to Substances Hazardous to Health, or 50 years for anything concerning radiation; although the Company reserves the right to retain Health Records in perpetuity, as the symptoms associated with some conditions may take a long time to present and there is no time limit on the raising of disability discrimination claims.

i. Records of any 'mining' for CV's from the Internet will be kept for no more than one month unless Explicit Consent is obtained.

j. CCTV images are automatically deleted after three weeks.

Secure Destruction

All data which is to be disposed of must be destroyed securely.

Vehicle Trackers/CCTV/Site Entry Systems

Company Vehicles are fitted with tracker devices; and this and our right to use Tracker Data/Records is stated in the Company's Privacy Notice to Employees, Agency Workers, Subcontractors, etc. It is also stated in other documentation given to all new employees (including Offer Letters/Handbook) and is therefore a condition precedent to the employment contract, contract of service, etc.

The Company therefore has the right to use Tracker Data/Reports for lawful purposes including but not limited to:-

a. verifying times on/off site,
b. in support of the Company's contractual claims against its clients,
c. bringing/resisting/defending any claim in a Court/Arbitration/Adjudication/Tribunal or in defending any prosecution,
d. in conjunction with the Company's Disciplinary Procedure, and/or
e. to properly calculate wage/salary/fee payments due.

Entry to many of our clients' Sites is controlled by Digital Entry/Sign-In Systems; and the Company is therefore obliged to instruct all Employees, Agency Workers & Subcontractors who attend such site(s) to undergo the process which is in place. Such Systems commonly involve the use of retinal scan, fingerprinting, etc. Complying with our client's system is necessary for the performance of the Company's obligations under contracts of employment, service, etc. with Data Subjects.

The Company currently uses CCTV in certain of its premises in order to prevent/detect fraud, theft, etc. Wherever a Data Subject can be identified, images will be processed as Data in accordance with this Policy and with GDPR. Such images are automatically deleted after three weeks.

Other

The Company does not carry out automated decision-making.

Data may be stored in 'the cloud' and this will be hosted by Microsoft based within the EU; which is generally regarded as being GDPR-compliant. Other than that, Data will not normally be transferred abroad.

However, GDPR permits Data transfer to other countries inside or outside the EU where the transfer is necessary for the performance of a contract of employment/service (e.g. where a Data Subject has raised a grievance, in the course of a disciplinary procedure, where a contractual query has been raised/improved terms have been requested, etc., and a key Director/Manager/Consultant is temporarily out of the UK). Any movement of Data abroad will be carried out with appropriate protection.

The Company will never sell Data relating to individuals or share it with third parties other than for a lawful purpose referred to herein.

Author: Richard Essam, Commercial Director
For and on behalf of The Directors of Graham Holmes Astraseal Ltd
Date: 25.05.18