DATA PRIVACY, PROTECTION AND MONITORING POLICY

This Policy refers to the ARG GROUP. The ARG GROUP is the name given to the collective companies ARG EUROPE, ARG CONTRACTS, ARG SURVEYS. This Policy applies to all under the ARG GROUP Banner.

Who does this policy apply to?
Everyone working within the ARG Group. This includes all employees and temporary workers employed through a third party i.e. Sub-Contractors.

Also, as this policy isn't part of our contracts, we're able to change it if we need to from time to time.

Why do we have this policy?
It's important to us that everyone working for or with us understands what we do, and what they need to do, to make sure that we keep data safe and protected, in line with Data Protection law. We are committed to all aspects of Data Protection under the Data Protection Act 1988 and the General Data Protection Regulations 2016/679 (GDPR). This policy sets out how the organisation deals with personal data including personnel files and data subject access requests and employee obligations in relations to personal data of all shareholders (Employees, Clients, Contractors, Residents).

Data Protection Officer, Controller and Processor
The responsibility for the implementation of this policy sits with the Managing Director, Chris Blair, as Data Protection Officer and 'Controller' with the Compliance Manger, Victoria Blair, acting as deputy.

The GDPR applies to 'controllers' and 'processors'.

- A controller determines the purposes and means of processing personal data.
- A processor is responsible for processing personal data on behalf of a controller.
- If you are a processor, the GDPR places specific legal obligations on you; for example, you are required to maintain records of personal data and processing activities. You will have legal liability if you are responsible for a breach.
- However, if you are a controller, you are not relieved of your obligations where a processor is involved – the GDPR places further obligations on you to ensure your contracts with processors comply with the GDPR.

Everyone working for or on behalf of the ARG Group are classed as 'Processors'.

If you have any questions about the policy then please contact your line manager in the first instance and they will be able to forward your query on if required.

DATA PRIVACY, PROTECTION AND MONITORING POLICY

What data is covered?

In this policy the data we're talking about is information about people, (the person the data's about is known as the 'data subject') and includes opinions or intentions towards them. For data to be covered, it needs to be recorded and used electronically (e.g. on a computer) or, if on paper, it needs to be kept in a structured and indexed manual file (e.g. personnel file). However when storing the data, it needs to be kept securely (e.g. if it's stored electronically it should be password protected; if it's a paper copy it should be stored where only the right people can access it).

For more information on information security please read the *'INFORMATION SECURITY POLICY'*

Under GDPR data also includes: Online Identifiers, Location Data, Socioeconomic and genetic data.

How does the ARG Group comply with the law?

We need to make sure that you read and understand this policy (and if you're a manager make sure your teams do so too). Also, there are eight principles that we have to follow under the law:

1. We need to process data fairly and lawfully: This means that we should only process data for one or more of the following reasons;
    a. We have a business reason to do it
    b. We need to do it so we can meet our responsibilities under a contract that we have with the person (or their company)
    c. The person has said they're happy for us to do it (e.g. ticked a consent form)
    d. Legally we have to (e.g. tax information, statutory audits, and government enforcement agencies)
    e. We need to so that we can protect the person
    f. We need to so that a legal process can take place (e.g. court proceedings)
2. We need to use data only for what we've said we'll use it for
3. We need to make sure that we have enough, but not too much, data for what we're using it for and that it's relevant to what we're using it for
4. We must hold accurate data
5. We have to make sure that we only keep data for the time that we actually need it
6. We have to handle any data in a way that doesn't breach people's Data Protection rights
7. We need to keep all data safe and secure
8. If we're sending data outside of the European Economic Area (EEA), we need to make sure that it's properly protected to do this.

Sensitive personal data is information about racial or ethnic origin, political opinions, religious beliefs (or beliefs of a similar nature), membership of a trade union, health conditions, sexual

orientation, criminal records (or allegations) or details of legal proceedings. Information about these things should be more restricted (e.g. with an extra password). It should only be accessed on a 'need to know' basis and should be kept by HR (and sometimes Payroll).

The Information Commissioner's Office (official, legal body) also has power to; issue information notices to us (i.e. tell us we have to give them certain information), issue enforcement notices to us (i.e. make us do certain things so that we comply with the law), come and inspect our premises (powers of entry).

What if I want to know what information the ARG Group has about me?
You can make a 'Data Subject Access Request' to your line manager or contact at ARG and ARG Group's Data Protection Officer (Chris Blair) will be informed of your request. If you make a request you'll need to be specific about the information you want and where it's kept.

You have a right to rectification of your data, therefore If you are aware that the information we are holding is either incorrect or inaccurate you have the right to request that this information is rectified

I work for the ARG Group, What's held on my personnel file?
All staff have a personnel file this may be held electronically or paper based. In this file it will have information about your work history e.g. absences, disciplinary, grievances, starter's information's, references, performance information NI details, address details.
There may also be other information about you located within the organisation, for example your manager's inbox or desktop, with payroll, or HR, or within documents stored in a relevant filing system.

We may from time to time collect relevant sensitive personal information from you for equal opportunities monitoring purposes or for the purpose of government level clearance checks.

Any personal information will be securely stored at all times. Any hard copies of personal information will be stored securely in locked filing cupboards or cabinets and information stored electronically will be subject to access controls and passwords and encryption software will be used where necessary.

Where laptops, Tablets and Company phones, that may hold personal information, are taken off site, employees must follow the organisation's relevant policies relating to the security of information.

As a CRM system we currently use EASYBOP, information on this is password accessible and the data individuals can see is limited to their job roles.

DATA PRIVACY, PROTECTION AND MONITORING POLICY

I work or have worked for the ARG Group, How long do you keep my information for if I leave the company?

If you leave the company we will archive your information in a secure area (this means somewhere no one can access, and still has the above protection) and we will keep your records for a maximum of 12 years. After this we will destroy all the information that we have relating to you with the exception of Medical and Exposure records which by law must be kept for a minimum of 40 Years or until your 80th Birthday (whichever comes first)

What happens if I don't follow the policy?

Breaching this policy could lead to disciplinary action (including dismissal) and in the very worst cases prosecution, leading to an unlimited fine.

Who do I contact if I have a question or complaint about Data Protection?

ARG Group's Data Protection Officer.

Will there be any training on Data Protection?

Yes, ARG Group will look to provide relevant training on data protection issues to all staff who handle personal information at work. The organisation will continue to provide such employees with refresher training on a regular basis where required.

Does ARG Group carry out any Monitoring?

Yes, at times we may choose to monitor our staff by various methods this may include CCTV, checking emails, IM's, phone and internet usage including mobiles, listening to voicemails and monitoring telephone conversations.

All ARG Group Company vans are fitted with Navman / Teletrac tracking which monitors the speed, location and movement of all vehicles. A weekly report is produced with information of all Company van movements. This includes start and finish times, dates driven and if you have broken the speed limit. This information may then be used for a disciplinary.

Any information that is collected through monitoring is stored safely and securely on our Company servers. We only hold this information for a maximum of 18 months, after this we destroy the files.

In exceptional circumstances, we may carry out covert monitoring. This may be appropriate where there is, or could be, damage caused to us. Covert monitoring will only take place with the approval of the Managing Director.

Signed: 

Role: Managing Director

Date: 1st May 2020