ATLAS SAFETY MANAGEMENT

Toolbox Talks

SAFETY ADVICE DESIGNED TO KEEP YOUR STAFF SAFE AND YOUR BUSINESS COMPLIANT

Data Protection Act

The Data Protection Act 2018 is the UK's implementation of the General Data Protection Regulation (GDPR).

Europe is now covered by the world's strongest data protection rules. The mutually agreed General Data Protection Regulation (GDPR) came into force on May 25, 2018 and was designed to modernise laws that protect the personal information of individuals.

Before GDPR started to be enforced, the previous data protection rules across Europe were first created during the 1990s and had struggled to keep pace with rapid technological changes. GDPR alters how businesses and public sector organisations can handle the information of their customers. It also boosts the rights of individuals and gives them more control over their information.

Main Points

Everyone responsible for using personal data has to follow strict rules called 'data protection principles. They must make sure the information is:

- used fairly, lawfully and transparently
- used for specified, explicit purposes
- used in a way that is adequate, relevant and limited to only what is necessary
- accurate and, where necessary, kept up to date
- kept for no longer than is necessary

handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage

There is stronger legal protection for more sensitive information, such as:

- race
- ethnic background
- political opinions
- religious beliefs
- trade union membership
- genetics
- biometrics (where used for identification)
- health
- sex life or orientation

There are separate safeguards for personal data relating to criminal convictions and offences.

Discussion Points

- **Myth 1**: The biggest threat to organisations from GDPR is massive fines
- **Fact**: This law is not about fines. It's about putting the consumer and citizen first.
- **Myth 2**: You must have consent if you want to process personal data
- **Fact**: The GDPR is raising the bar to a higher standard for consent.
- **Myth 3**: GDPR is an unnecessary burden on organisations
- **Fact**: The new regulations do demand more of organisations in terms of accountability for their use of personal data, and it enhances the existing rights of individuals.
- **Myth 4**: All personal data breaches will need to be reported to the ICO
- **Fact**: It will be mandatory to report a personal data breach under the GDPR but only if it's likely to result in a risk to people's rights and freedoms.
- **Myth 5**: All details need to be provided as soon as a personal data breach occurs
- **Fact**: If a personal data breach needs to be reported, it needs to happen without delay and, where feasible, not later than 72 hours after having become aware of it.
- **Myth 7**: Data breach reporting is all about punishing organisations
- **Fact**: The new law is designed to push companies and public bodies to step up their ability to detect and deter breaches. What is foremost in regulators' minds is not to punish the organisations, but to make them better equipped to deal with security vulnerabilities.