INDEPTH HYGIENE SERVICES
40 Years of Excellence

Data Protection & Privacy Policy

Indepth Hygiene requests and holds specific information about employees, contractors, suppliers and clients in the course of our business operations. This is limited to purpose, checked for accuracy, held securely, processed fairly and lawfully in line with an individual's rights then disposed of safely when no longer relevant or required. It will only be shared with third parties for legitimate business purposes such as but not limited to sub-contractors, lawyers, debt collection agencies, etc. and kept only as long as is justifiable under statutory, regulatory, legal or security reasons i.e. HMRC retention requirements.

An explanation of our lawful basis for processing and consent for retaining this data is included on all new contracts of employment and new account forms requested from prospective clients.

In line with the Data Protection Act 1998 & General Data Protection Regulation (GDPR) effective 25th May '18, data is stored in password protected areas of an in-house computer system, accessible by authorised personnel or departments specific to its use. Where printed documents are required these are kept in locked cabinets with limited keyholders appointed according to their role's specific requirement for that data. The offices have a 24/7 police-monitored alarm system & are kept locked at all times, accessible via coded keypad entry during office hours or to keyholders only, with visitors kept to a minimum and accompanied at all times. Roles requiring remote working are limited to accessing relevant data only via password protected equipment and are required to be additionally aware of any unauthorised persons nearby when accessing.

Data subjects have a right of access and correction of any information held about them and are requested to email admin@indepthhygiene.co.uk should they wish to exercise either of these rights, and informed of their right to complain to the ICO should they suspect a problem with the way we are handling their data. Access requests will be responded to within 28 days.

Any breaches in data security, monitored continuously by our external IT specialists, will be notified to relevant personnel/clients within 72 hours.

When personal data is no longer required it is deleted from all computer-based systems by the relevant department and any documentation containing same shredded. As an additional precautionary measure, hard drives are certifiably wiped of all remaining data on disposal and any remaining paperwork regularly and certifiably shredded by external consultants.

This policy is communicated and explained to all employees by their Line Manager as they are expected to comply with all requirements and are actively involved in its ongoing implementation and reporting of any known breaches or non-conformance.

Whilst formal designation of a Data Protection Officer (DPO) is not required for our organisation, Senior Management are committed to complying with the requirements of Data Protection by Design with the HR/Finance Director holding a Certificate of Continuing Professional Development for GDPR and the Managing Director taking responsibility for reviewing the company's compliance with this policy and identifying any areas for improvement. The policy itself will be reviewed annually by senior management to ensure continued suitability.

R M Norman – Managing Director - March 2018