Guild of Cleaners and Launderers

GUILD OF CLEANERS & LAUNDERERS

For A Better Qualification Choose the Guild of Cleaners and Launderers

May 2018 E-Bulletin

This May Issue is two pages due to GDPR and the complexities in explanation

Intermediate Laundry Technology a weeks intensive training course held once per year. Very popular in the past and we are currently planning our next. Please register your interest as we require 10 delegates to make the training viable. Contact enquiries@gcl.org.uk or telephone 01698322669 to book places.

Guild Membership Renewal? Your Membership Subscription for the year 2018/19 was due from the beginning of April and if not already paid remember that you can now pay on line by visiting the Guild Website at www.gcl.org.uk, or alternatively, Telephone 01698 322669 . Paying on time saves money and time in having to check and chase late payers. Contact enquiries@gcl.org.uk

Guild Web Site has been upgraded visit http://gcl.org.uk to see what a difference we have made.

Now with ReportCam—see the website for more details

See this month a Technical Bulletin dealing with Safety in Textile Care and an Amber Alert dealing with a Shirt Purchased at Harrods

Guild and General Data Protection Regulation (GDPR) Your Guild has reviewed systems to ensure compliance

Guild of Cleaners and Launderers

56 Maple Drive,
Larkhall, South Lanarkshire,
ML9 2AR

Phone: 01698 322669
E-mail: enquiries@gcl.org.uk

General Data Protection Regulation (GDPR)

GDPR is designed to give individuals better control over their personal data held by organisations, and Personal Data is defined as any information relating to a person who can be identified directly or indirectly. This includes online identifiers, such as IP addresses and cookies, if they are capable of being linked back to the data subject.

Indirect information might include physical, physiological, genetic, mental, economic, cultural or social identities that can be linked back to a specific individual.
There is no distinction between personal data about an individual in their private, public or work roles all are covered by this regulation. Some larger companies may need to appoint a Data Protection Officer as a result of this new regulation even if only a temporary appointment.
There will be a substantial increase in fines for organisations that do not comply with this new regulation. Penalties can be levied up to the greater of ten million Euros or two per cent of global gross turnover for violations of record-keeping, security, breach notification and privacy impact assessment obligations. These penalties are doubled to twenty million Euros or four per cent of turnover for violations related to legal justification for processing, lack of consent, data subject rights and cross--border data transfers. Indirect information might include physical, physiological, genetic, mental, economic, cultural or social identities that can be linked back to a specific individual. There is no distinction between personal data about an individual in their private, public or work roles – all are covered by this regulation.
Companies will be required to "implement appropriate technical and organisational measures" in relation to the nature, scope, context and purposes of their handling and processing of personal data. Data protection safeguards must be designed into products and services from the earliest stages of development.
These safeguards must be appropriate to the degree of risk associated with the data held and might include:• Pseudonymisation and/or encryption of personal data• Ensuring the ongoing confidentiality, integrity, availability and resilience of systems • Restoring the availability of, and access to, data in a timely manner following a physical or technical incident• Introducing a process for regularly testing, assessing and evaluating the effectiveness of these systems.
A key part of the regulation requires consent to be given by the individual whose data is held. Consent means "any freely given, specific, informed and unambiguous indication of his or her wishes by which the data subject, either by statement or by a clear affirmative action, signifies agreement to personal data relating to them being processed".
Organisations will need to be able to show how and when consent was obtained. This consent does not need to be explicitly given, it can be implied by the person's relationship with the company. However, the data obtained must be for specific, explicit and legitimate purposes. Individuals must be able to withdraw consent at any time and have a right to be forgotten; if their data is no longer required for the reasons for which it was collected, it must be erased.
When companies obtain data from an individual, some of the areas that must be made clear are:
• The identity and contact details of the organisation
• The purpose of acquiring the data and how it will be used
• Whether the data will be transferred internationally
• The period for which the data will be stored
• The right to access, rectify or erase the data
• The right to withdraw consent at any time
• The regulations demand that individuals must have full access to information on how their data is processed and this information should be available in a clear and understandable way. Individuals can make requests, and these must be executed "without undue delay and at the latest within one month of receipt of the request". Where requests to access data are manifestly unfounded or excessive then small and medium-sized enterprises will be able to charge a fee for providing access.

Continued on page 2

See page two for the Guild's Compliance to GDPR

Continued from page 1

Companies must report breaches of security “leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed”.
In the event of a personal-data breach, companies must notify the appropriate supervisory authority “without undue delay and, where feasible, not later than 72 hours after having become aware of it” if the breach is likely to “result in a risk for the rights and freedoms of individuals”.
In March 2016, the UK Information Commissioner’s Office (ICO) published Preparing for the General Data Protection Regulation (GDPR) – 12 Steps to Take Now. Nine of these steps for organisations are

1. Ensure key departments are aware that the law is changing, and anticipate the impact of GDPR.
2. Document what personal data is held, where it came from and with whom it is shared.
3. Review current privacy notices, and make any necessary changes.
4. Review procedures to address the new rights that individuals will have.
5. Plan how to handle requests within the new time frames, and provide the required information.
6. Identify and document the legal basis for each type of data processing activity.
7. Review how consent is sought, obtained and recorded.
8. Make sure procedures are in place to detect, report and investigate data breaches.
9. Designate a Data Protection Officer to take responsibility for data protection compliance if the company is large enough or the system used requires this level of activity.

It is possible any information stored on your counter computerised e-pos system may contravene the regulation but it depends on how you use the details of the customers. If you hold personal data in some form, such as customer databases or employee payroll records then this affects you and you must act to conform and also make your employees aware of the responsibility.

If they freely share their details with you and you do not pass on to any other party that information then you are not in contravention if that information is stored only on your system and it is not accessible by anyone other than yourselves. If the counter epos system is a version where information is stored elsewhere then you must ascertain if this data is secure, or can it be accessed by a third party. The regulation is trying to stop personal data being used without authority and if you use it only in order to carry out the transaction between yourself and the customer, and that they willingly shared this with you, then you will comply, provided you take steps to ensure no one else has access to it, or that you do not share it, for any reason, with a third party without the customer's consent. Make others in your business aware of the new regulation.

The Guild of Cleaners and Launderers and GDPR

Your Guild has looked at the requirements of the new regulation and our general compliance in relation to our members.

Members Personal Information received is not shared with any other individual or organisation and although we have members overseas the files we keep are secure and never shared overseas.

Members have access to their personal data via the Guild’s website and can update, or erase, this information at any time by visiting the site and logging on to their data via their own personal pin number, which is not known by, or shared with any Guild official. However, if this data is changed, or deleted, please advise the Guild secretariat because they have no access to these records and changes made may have implications on future contact with you the member.

It is condition of membership that we keep certain personal member details for example to contact members and share relevant information with them, but this has always been secure and never shared.