5 answers to give when a client asks if you are GDPR compliant

ISO Systems UK

Intelligent Management Systems

Practical, Simple & Flexible

5 answers to give when a client asks if you are GDPR compliant

GDPR compliance is a complex state to achieve. It is not something that you do once and then you are compliant. It is an ongoing process and entails many changes to an organisation and how it functions, not just in the IT area as many people think.

GDPR compliance covers areas of consent management, direct marketing to existing and new clients, human resources management and employee information, as well as information use and security, staff training, access requests and breach management.

In addition very few organisations will be 100% compliant 100% of the time, the real challenge is to be maintaining a program of compliance. So, when a client asks you, **"Are you compliant with the GDPR regulations?" a simple YES or NO answer is not really possible**.To answer the question, you give at least 5 answers.

Here is how we suggest you answer the question. GDPR compliance requires an ongoing program to manage and maintain. GDPR compliance is not a once off event, it is a series of action required in order to conform with regulations, which you must review on a periodic basis to ensure that maximum compliance is attained.

We have a program in place to manage these actions and tasks as well as review and rectify our compliance status where necessary.

Answer 1 – We manage our compliance within the main compliance areas of Consent, Marketing, Human Resources and Information use and security as follows:

Consent management – We ensure we have a lawful basis for obtaining consent from people by ensuring they perform a clear affirming act, give consent freely, unambiguously and for specific purposes. We understand that consent can be withdrawn at any point. We review our compliance on a quarterly basis to ensure its ongoing. This is in line with Article 7 of the GDPR regulation.

Marketing– We manage our marketing compliance in the three main areas of marketing, to existing clients, to prospective clients and in terms of profiling clients. We actively seek consent for all activities and comply with the GDPR guidelines for marketing activities. We review our compliance with the GDPR in terms of our marketing activities on a quarterly basis.

Human Resources – We are constantly vigilant in our collection and management of the personal and sensitive personal information of employees as well as prospective employees. We manage the information in the following categories, recruitment information, employment records and employee health information using the GDPR as our guide. In addition where we monitor employees we perform a data protection impact assessment to justify the monitoring. All our employees are fully aware of what we do and how we manage the employees and we have a valid employee privacy notice. We review our compliance on a quarterly basis.

Information use and security – We understand that information stored on IT infrastructure or moving between infrastructure is highly vulnerable. We ensure that we manage information in terms of retention and restriction, use of information technology, information quality and we have appropriate security controls. We use the GDPR as our guide along with other procedures such as ISO 270001. We review our security controls on a monthly basis and our other aspects of information use and security on a quarterly basis.

Answer 2 – We have relevant privacy notices and have a procedure for managing subject access requests. We also have policies in place covering a number of privacy requirements.

We have mapped our usage of personal and sensitive personal information with all the relevant types of people we interact with, the reason we interact with them, the information both personal and sensitive (with further legal basis) we collect and use as well as where we process and store the information, including in house and external processor locations. We have policy and training documents available and communicated to our staff covering the areas of:

- Employee training
- Data Protection Policy
- Employee Privacy Notice
- CCTV Policy (where relevant)
- Information classification and labelling standard
- Information protection and handling policy
- Third country transfers
- And any others you may have…

We have created our records of processing activities and should there be major changes to these we will conduct a data protection impact analysis.

Answer 3 – Our employees are aware and trained about our privacy policies on an ongoing basis.

We have procedures in place to inform all employees of our policies and to monitor that they have read and accepted these. New employees are informed about policies as part of their onboarding procedures.

Answer 4 – We manage the organisations to who we outsource various processing purposes.

We ensure that we have processor agreements with the organisations we outsource any processing of personal or sensitive personal information to. We ensure via a relevant processor agreement that they conform with our requirements and the requirements of the GDPR. We review our processor contracts prior their expiry and ensure no organisation can perform processes for us without having the relevant contracts in place. We understand that we are jointly and severally liable in the case of a processor organisation being breached and our information being threatened or abused.

Answer 5 – We have a record of all subject access requests and breaches which have occurred in our organisation and we respond to these and report these where relevant.

We have a mechanism in place to receive and process requests from people about the information that is held about them. We will respond to these requests in the timescales outlined by the GDPR. We keep a register of all such requests made. We record all breaches that have occurred of whatever nature and these are reported to the supervisory authorities if required to within 72 hours. The above content serves as a guide to show what is required in order to be compliant with the GDPR regulation and to enable the communication of compliance to other parties. It is an example and should not be used as a final document.