GDPR and how it affects Mystery Shopping

GDPR legislation became enforceable on 25th May 2018.

What is GDPR?

The **General Data Protection Regulation (GDPR)** (Regulation (EU) 2016/679) is a regulation by which the European Parliament, the Council of the European Union and the European Commission intend to strengthen and unify data protection for all individuals within the European Union (EU).
GDPR provides the requirements for the protection of personal data. It seeks to **harmonise data privacy laws** across Europe and gives greater protection and rights to individuals. It changes how businesses and public organisations process and store data. Failure to comply could mean **financial penalties of up to 4%** of a company's global prior year **annual revenue**.

Why was it introduced?

The regulation is designed to meet the needs of the 21st century. The amount of digital information we create, capture and store has grown exponentially as consumers and businesses take advantage of the opportunities offered by the digital economy. The misuse of data by businesses and government has started to create public distrust.

How does it apply – What are Data Controllers and Data Processors?

GDPR applies to any business that deals with personal data of an EU resident, regardless of where that business is located.

The regulation applies to the **Data Controller**:

- The body which determines the legal basis, purposes and means of processing personal data
- A Mystery Shopping Provider is a **Data Controller** of the data relating to data subjects such as **their employees** and **their Mystery Shoppers**
- A Data Controller may use a Data Processor to work with personal data.

The regulation also applies to the **Data Processor**:

- A body that processes personal data on behalf of a Data Controller
- A Mystery Shopping Provider is a **Data Processor** on behalf of their **clients**, who are the Data Controllers for their employees (e.g. staff and network) and their channels (independent dealers and/or franchised network)
- A supplier of systems or services that enable a Mystery Shopping Provider to operate is also a **Data Processor** (e.g. a software supplier or fieldwork partner).

Who are the "Data Subjects"?

Data subjects are the individuals whose data you collect and process for the defined purpose(s) of your business.
The following is a list of potential data subjects as they apply to Mystery Shopping only:

For Storecheckers as a Data Processor (on behalf of our clients)	**For Storecheckers as a Data Controller**
Our clients Employees	

People we may Mystery Shop	Our Employees
People we report results to*	Our Mystery Shoppers
Our clients dealer or franchise employees	Our suppliers
People we may Mystery Shop	Our clients
People we report results to*	
* Also potential Data Recipients	

What is their "Personal Data"?

"Data" includes both **personal data** – broadly defined as a piece of information that can be used to identify an individual such as a name or IP address – and **sensitive personal data** such as religious and political views or sexual orientation.

In the case of Mystery Shopping the following are examples of data that is Personal or Sensitive for us as a Data Controller. More details regarding personal data and special categories can be found in Article 9 (1) of the GDPR regulations:

In the case of Mystery Shopping the following are examples of data that is Personal or Sensitive as a Data Processor on behalf of a Client (Data Controller) *NB.More details regarding personal data and special categories can be found in Article 9 (1) of the GDPR regulations:*

Employees (or channel employees) who are potential subjects of a Mystery Shop

Personal Data - name, gender, age approximation, physical description.

Sensitive Personal Data - religious, political or sexual orientation

Employees (or channel employees) who are recipients of Mystery Shop reports

Personal Data - name, gender, location, email details

Sensitive Personal Data - religious, political or sexual orientation

How does the regulation protect the Data Subject?

The regulation protects data subjects from the illegitimate use, misuse or disclosure of personal information either intentionally or as the victim of a data breach.
In effect, GDPR gives power back to the data subject.
A data subject has the right of full transparency and protection of their data.

GDPR gives data Subjects the following rights;

Consent - Agree or disagree to their data being processed – it is the responsibility of the **Data Controller** to seek this consent (ie Storecheckers)
Review - the personal data held.
Correct - the personal data held
Erase – demand the complete removal of personal and/or sensitive data (Right to be forgotten, Article 13 GDPR)
Be Informed – in the event of a hack or data loss or theft. Controllers and Processors must notify their local data protection regulator.