CODE OF CONDUCT

Implementing GDPR

H-S-R-L
HIGHWAY STOPS RETAIL LIMITED

Highway Stops retail Ltd Unit 11 Metro Trading Centre, Second Way, Wembley, Middlesex, HA9 0YJ Tele:-020 8900 0181

February 2019

Code of Conduct

Handling Client Personal and Sensitive Data

General Data Protection Regulation

The purpose of this Code of Conduct is to inform all the members of staff and management of Highway Stops Retail Ltd on process and handling of personal/sensitive data relating to individuals according to the basic terms of Regulation (EU) 2016/679 This manual can be read as part of the Highway Stops Retail Ltd's General Data Protection Policy.

CODE OF CONDUCT

Handling Customers Personal Data

According to the European Union's Regulation (EU) 2016/679, known as the General Data Protection Regulation ('GDPR'), regulates the processing by an individual, a company or an organisation of personal data relating to individuals in the EU.

Personal Data means any information/data relating to an identified or identifiable natural person ('Data Subject');

An identifiable person is one who may identified, either directly or indirectly, in particular by reference to the full name, an identification number, passport number, social insurance number, address or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity. Any or part of data which is collected together can lead to the identification of a person, that constitute personal data.

The regulation applies to natural persons in the course of a professional activity, such as the employees of a company/organisation, e.g. business email addresses or employees' business telephone numbers. The regulation does not apply either to deceased persons or legal entities. Data provided anonymous which is not identifiable is not data. Furthermore the regulation does not apply either for private or personal reasons. In such cases the data should not be processed at all. It applies only for professional and/or business activities. Encrypted data may be used to identify a person's data.

Data may be provided or collected either on paper, or through IT system, or through CCTV (Video surveillance systems).

An example of personal data

The following General Personal data may be collected and processed:

1. Full name and surname
2. Home Address
3. Telephone/ Mobile/Email
4. National Insurance Number/ Passport
5. Social Insurance Number
6. Internet Protocol (IP) address
7. A cookie ID
8. Posting Personal photo
9. And any other personal information

The process of the above data may include (wholly or partly automated) from collection, recording, structure, storage, alteration, recovery, use it, disclosure, transmission, deletion.

The current Code of conduct helps you to understand the regulation, and how you process of such data:

(a) Processed lawfully, fairly and in a transparent manner in relation to individuals;

(b) Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

(c) Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

(d) Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that Personal Data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

(e) Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the Personal Data are processed; Personal Data may be stored for longer periods in so far as the Personal Data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organizational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and;

(f) Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures;

Any personal Data shall not be transferred to any country outside the European Economic Area unless that country ensures and has adequate level of protection for the rights and freedoms of "data subjects" in relation to the processing of personal data.

Therefore certain important guidelines and rules to follow:

- Everyone handling and managing Personal Data understands(data controller + data processor) that they are contractually responsible for following good data protection practice;
- Everyone managing and handling Personal Data is appropriately trained to do so;
- Everyone managing and handling Personal Data is appropriately supervised;
- anybody wanting to make enquiries about handling personal Information knows what to do;
- Queries about handling Personal Data are promptly and courteously dealt with;
- methods of handling Personal Data are clearly described;
- Regular review and audit is made of the way Personal Data is managed, including CCTV systems.
- Methods of handling Personal Data are regularly assessed and evaluated;
- Regular assessment for compliance with the GDPR/Data Protection will take place.

Article 6(1) of GDPR setsoutthefollowing lawful basesforprocessing;

- The Data Controller has to comply with a legal obligation to which the Controller is subject.
- The processing is necessary for the performance of a contract to which the data subject is a party, or steps prior to entering a contract with a data subject.
- The processing is necessary for the purposes of legitimate interests pursued by the Data Controller or third party.
- The Data Subject has given their consent to the processing
- The processing is necessary to protect the vital interests of the Data Subject
- The processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Data Controller.

Period of time the Data is kept

You must store data for the **shortest time possible**. That period should take into account the reasons why your company/organisation needs to process the data, as well as any legal obligations to keep the data for a fixed period of time (for example national labour, tax or anti-fraud laws requiring you to keep personal data about your employees for a defined period, product warranty duration, etc.).

Your company/organisation should establish **time limits** to **erase or review** the data stored.

By way of an exception, personal data may be kept for a longer period for archiving purposes in the public interest or for reasons of scientific or historical research, provided that appropriate technical and organisational measures are put in place (such as anonymisation, encryption, etc.).

Your company/organisation must also ensure that the data held is accurate and kept up-to-date.

Examples of processing

Examples of processing

1. customer order taking and processing
2. profiling of customers
3. vendor management
4. service provision through contractors
5. staff management and payroll administration;
6. access to/consultation of a contacts database containing personal data;
7. sending promotional emails;
8. shredding documents containing personal data;
9. posting/putting a photo of a person on a website;
10. storing IP addresses or MAC addresses;
11. video recording and viewing (CCTV).

Whom does the data protection law apply to?

The law applies to:

1. A company or entity which processes personal data as part of the activities of one of its branches established in the EU, regardless of where the data is processed; or
2. A company established outside the EU offering goods/services (paid or for free) or monitoring the behaviour of individuals in the EU.

Do the data protection rules apply to data about a company?

No, the rules only apply to personal data about individuals; they do not govern data about companies or any other legal entities. However, information in relation to one-person companies may constitute personal data where it allows the identification of a natural person. The rules also apply to all personal data relating to natural persons in the course of a professional activity, such as the employees of an organisation, business email addresses or employees' business telephone numbers.

What data can we process and under which conditions?

The type and amount of personal data you may process depends on the reason you are processing it (legal reason used) and what you want to do with it. You must respect several key rules, including

1. Personal data must be processed in a lawful and transparent manner, ensuring fairness towards the individuals whose personal data you are processing ('lawfulness, fairness and transparency').
2. You must have specific purposes for processing the data and you must indicate those purposes to individuals when collecting their personal data. You cannot simply collect personal data for undefined purposes ('purpose limitation').
3. You must collect and process only the personal data that is necessary to fulfil that purpose ('data minimisation').
4. You must ensure the personal data is accurate and up-to-date, having regard to the purposes for which it is processed, and correct it if not ('accuracy').
5. You cannot further use the personal data for other purposes that are not compatible with the original purpose of collection.
6. You must ensure that personal data is stored for no longer, than necessary for the purposes for which it was collected ('storage limitation').
7. You must install appropriate technical and organisational safeguards that ensure the security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technology ('integrity and confidentiality').

Can data be processed for any purpose?

No. The purpose for processing of personal data must be known and the individuals whose data you are processing must be informed. It is not possible to simply indicate that personal data will be collected and processed. This is known as the 'purpose limitation' principle.

Can we use data for another purpose?

Yes, but only in some cases. If your company/organisation has collected data on the basis of legitimate interest, a contract or vital interests it can be used for another purpose but only after checking that the new purpose is compatible with the original purpose.

The following points should be considered:

1. The link between the original purpose and the new/upcoming purpose;
2. The context in which the data was collected (what is the relationship between your company/organisation and the individual?);
3. The type and nature of the data (is it sensitive?);
4. The possible consequences of the intended further processing (how will it impact the individual?);
5. The existence of appropriate safeguards (such as encryption or pseudonymisation).

If your company/organisation wants to use the data for statistics or for scientific research it is not necessary to run the compatibility test.

If your company/organisation has collected the data on the basis of consent or following a legal requirement, no further processing beyond what is covered by the original consent or the provisions of the law is possible. Further processing would require obtaining new consent or a new legal basis[1].

[1]Articles 5(1)(b), 6(4) and 89(1) and Recitals (39) and (50) of the GDPR

For how long can data be kept and is it necessary to update it?

You must store data for the shortest time possible. That period should take into account the reasons why your company/organisation needs to process the data, as well as any legal obligations to keep the data for a fixed period of time (for example national labour, tax or anti-fraud laws requiring you to keep personal data about your employees for a defined period, product warranty duration, etc.).

Your company/organisation should establish time limits to erase or review the data stored.

By way of an exception, personal data may be kept for a longer period for archiving purposes in the public interest or for reasons of scientific or historical research, provided that appropriate technical and organisational measures are put in place (such as anonymisation, encryption, etc.).

Your company/organisation must also ensure that the data held is accurate and kept up-to-date[2]

[2]Article 5(1)(e) and Recital (39) of the GDPR

What information must be given to individuals whose data is collected?

At the time of collecting their data, people must be informed clearly about at least:

1. Who your company/organisation is (your contact details, and those of your DPO if any);
2. Why your company/organisation will be using their personal data (purposes);
3. The categories of personal data concerned;
4. The legal justification for processing their data;
5. For how long the data will be kept;
6. Who else might receive it;
7. Whether their personal data will be transferred to a recipient outside the EU;
8. That they have a right to a copy of the data (right to access personal data) and other basic rights in the field of data protection (see complete list of rights);
9. Their right to lodge a complaint with a Data Protection Authority (DPA);
10. Their right to withdraw consent at any time;
11. Where applicable, the existence of automated decision-making and the logic involved, including the consequences thereof.

The information may be provided in writing, orally at the request of the individual when identity of that person is proven by other means, or by electronic means, where appropriate. Your company/organisation must do that in a concise, transparent, intelligible and easily accessible way, in clear and plain language and free of charge.

When data is obtained from another company/organisation, your company/organisation should provide the information listed above to the person concerned at the latest within 1 month after your company obtained the personal data; or, in case your company/organisation communicates with the individual, when the data is used to communicate with them; or, if a disclosure to another company is envisaged, when the personal data was first disclosed[3].

[3]Article 12(1), (5) and (7), Articles 13 and 14 and Recitals (58) to (62) of the GDPR

What personal data is considered sensitive?

The following personal data is considered 'sensitive' and is subject to specific processing conditions[4]:

1. Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs;
2. Trade-union membership;
3. Genetic data, biometric data processed solely to identify a human being;
4. Health-related data;
5. Data concerning a person's sex life or sexual orientation.

[4]Article 4(13), (14) and (15) and Article 9 and Recitals (51) to (56) of the GDPR

Under what conditions can my company/organisation process sensitive data?

Your company/organisation can only process sensitive data if one of the following conditions is met:

1. The explicit consent of the individual was obtained (a law may rule out this option in certain cases);
2. An EU or national law or a collective agreement, requires your company/organisation to process the data to comply with its obligations and rights, and those of the individuals, in the fields of employment, social security and social protection law;
3. The vital interests of the person, or of a person physically or legally incapable of giving consent, are at stake;
4. You are a foundation, association or other not-for-profit body with a political, philosophical, religious or trade union aim, processing data about its members or about people in regular contact with the organisation;
5. The personal data was manifestly made public by the individual;
6. The data is required for the establishment, exercise or defence of legal claims;
7. The data is processed for reasons of substantial public interest on the basis of EU or national law;
8. The data is processed for the purposes of preventive or occupational medicine, assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment, or the management of health or social care systems and services on the basis of EU or national law, or on the basis of a contract as a health professional;
9. The data is processed for reasons of public interest in the field of public health on the basis of EU or national law;
10. The data is processed for archiving, scientific or historical research purposes or statistical purposes on the basis of EU or national law.

Are there any specific safeguards for data about children?

Your company/organisation can only process a child's personal data on grounds of consent with the explicit consent of their parent or guardian up to a certain age. In UK, according to the law the, childbased on the child's consent to the processing of personal data if the child is at least fourteen (14) years old. A child under the age of fourteen (14), the consent is required provided or approved by the person having parental responsibility for the child.

How do we deal with requests from individuals exercising their data protection rights?

Individuals may contact your company/organisation to exercise their rights under the GDPR (rights of access, rectification, erasure, portability, etc.). Where personal data is processed by electronic means, your company/organisation should provide means for requests to be made electronically. Your company/organisation must reply to their request without undue delay, and in principle within 1 month of the receipt of the request.

It can ask them for additional information in order to confirm the identity of the person making the request.

If your company/organisation rejects the request then it has to inform the person of the reasons for doing so and of their right to file a complaint with the Data Protection Authority and to seek a judicial remedy.

Dealing with requests of individuals should be carried out free of charge. Where requests are manifestly unfounded or excessive, in particular because of their repetitive character, you may charge a reasonable fee or refuse to act.

What personal data and information can an individual access on request?

When someone requests access to their personal data, your company/organisation must:

1. Confirm whether or not it is processing personal data concerning them;
2. Provide a copy of the personal data it holds about them;
3. Provide information about the processing (such as purposes, categories of personal data, recipients, etc.)

Your company/organisation must provide the individual with a copy of their personal data free of charge. However, a reasonable fee can be charged for further copies.

The exercise of the right of access is closely linked to the exercise of the right to data portability – to allow the individual to transmit their data to another organisation.

What happens if someone objects to my company processing their personal data?

Individuals have the right to object to the processing of personal data for specific reasons. Whether such a specific situation exists must be examined on a case-by-case basis.

They may raise an objection only in cases where a public administration is processing the data in the context of its public tasks or when a company is processing the data on the basis of its legitimate interests. In such cases, your company/organisation may no longer process the data unless it demonstrates that it needs to process it for reasons that override the rights and freedoms of the individual or if the data is necessary for the establishment, exercise or defence of legal claims.

Individuals also have a right to object at any time to the processing of their personal data for direct marketing purposes. Direct marketing is understood under the General Data Protection Regulation as any action by a company to communicate advertising or marketing material, aimed at particular individuals. Your company/organisation must inform individuals in its privacy notice or at the latest at the time of the first communication with individuals, that it will be using their personal data for direct marketing and that they have a right to object free of charge. Where a person objects to processing for direct marketing purposes, your company/organisation may no longer process their personal data for such purposes.[5]

[5]European Commission: https://ec.europa.eu/info/law/law-topic/data-protection_en (accurate as of 14 February 2018)

What are the responsibilities of a Data Protection Officer (DPO)?

The DPO assists the controller or the processor in all issues relating to the protection of personal data. In particular, the DPO must:

1. Inform and advise the controller or processor, as well as their employees, of their obligations under data protection law;
2. Monitor compliance of the organisation with all legislation in relation to data protection, including in audits, awareness-raising activities as well as training of staff involved in processing operations;
3. Provide advice where a DPIA has been carried out and monitor its performance;
4. Act as a contact point for requests from individuals regarding the processing of their personal data and the exercise of their rights;
5. Cooperate with DPAs and act as a contact point for DPAs on issues relating to processing;

The organisation must involve the DPO in a timely manner. The DPO must not receive any instructions from the controller or processor for the exercise of their tasks. The DPO reports directly to the highest level of management of the organisation.

STAFF DATA PROTECTION GUIDELINES

1. Before collecting Client Personal Data (as defined above) we must receive clear and explicit instructions in any of the following methods:
   a. Engagement Letter
   b. Retainer
   c. Email
   d. Letter
   e. Oral instructions

2. All Client Personal Data (as defined above) must be stored with secure methods (both digital and hard-copy).
   a. Digital Client Personal Data must be saved only in secure folders where only the persons and/or team handling the case and the DPO have access.
   b. Hard-copy Client Personal Data must be saved in locked cabinets where only the persons handling the case and the DPO have access.
   c. Client Personal Data should not be left unattended / unsecured at any time.

3. Client Personal Data must be deleted / destroyed following a period of 7 years that the engagement has ended. Does not apply where we have a legal / professional / fiduciary duty to retain such Personal Data beyond the 7 year period.

4. Client Sensitive Data (as defined above) are never requested, unless necessary for services to be provided to the Client (i.e. Legal representation in matter relating to such sensitive information);

5. Client Personal Data is only transmitted to external partners who are regulated by a professional body (i.e. Auditors) and/or have signed a confidentiality agreement with CSP (i.e. external translators);

6. All members of staff ensure that a clean desk policy is implemented and no personal data or sensitive data is left unattended at any time;

7. All members of staff ensure that they log out from their PCs when leaving their desk and ensure that any mobile device is sufficiently password protected in case of loss;

8. All members of staff must ensure that they do not disclose to anyone their login details and/or passwords;

9. Client Personal Data are only transmitted outside the EU-USA where a Data Exchange Agreement has been signed with such entity who will be processing the Client personal data;

10. Client Personal Data are not be used for marketing and/or any other matters not relating to the services of CSP

11. Where Client objects to Marketing and/or Communication options, he must be deleted from all applicable marketing lists.

12. Transmission of Client Data on mobile and/or external devices (i.e. VPN, Email) is possible when essential to the provision of legal services but all appropriate security measures must be taken.

13. Transmission and/or transfer of Client Data through external storage devices (USB, hard drives, CD) is prohibited unless explicitly required for the purposes of providing services to the Client. Back-up storage of servers and client databases on external devices is permitted only with the permission of the IT Director and the DPO.