CitNOW

CitNOW Data Protection Policy

Last Updated:
July 2018

www.**citnow**.com

English Version

ZYPE TV LTD – DATA PROTECTION POLICY

ZYPE TV LTD - GDPR STATEMENT FOR CitNOW RETAILERS

Zype TV Ltd – Data Protection Policy

1. Policy Statement

1.1

All individuals have rights with regard to how their personal information is handled. During the course of our business activities we may collect, store and process personal information about our employees, suppliers and customers and we recognise the need to treat it in an appropriate and lawful manner. This Data Protection Policy covers our treatment of data belonging to our suppliers, customers and other third parties who we engage with. Our position with regard to employee data is set out in our Fair Processing Notice (Employee Data).

1.2

The information which we may receive, hold and process in respect of suppliers, customers and other third parties is subject to certain legal safeguards specified in the Privacy Law (meaning all applicable law relating to the processing of personal data including the Data Protection Act 1998, the General Data Protection Regulation 2016/679, the Privacy and Electronic Communications (EC Directive) Regulations 2003 and any statutory instrument, order rule or regulation made, as amended, extended, re-enacted or consolidated from time to time). The Privacy Law imposes restrictions on how we may use that information and we shall comply with the provisions of the Privacy Law at all times.

2. Status of the policy

2.1

This policy sets out our rules on data protection and the legal conditions that we will satisfy in relation to the obtaining, handling, processing, storage, transportation and destruction of personal information.

2.2

The Zype Data Protection Compliance Manager is responsible for ensuring compliance with Privacy Law and with this policy. Any questions or concerns about the operation of this policy should be referred in the first instance to the Data Protection Compliance Manager – Address: CitNOW, Millars Brook, Molly Millars Lane, Wokingham, Berkshire, RG41 2AD. Telephone: 0118 997 7740.

2.3
If you consider that this policy has not been followed in respect of personal data about yourself or others you should raise the matter with our Data Protection Compliance Manager.

3. Definition of data protection terms

3.1
Data is information that is stored electronically, on a computer, or in certain paper-based filing systems.

3.2
Data subjects for the purpose of this policy include all living individuals about whom we hold personal data. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal data.

3.3
Consent of the data subject, means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

3.4

Personal means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

3.5

Data controllers means the natural or legal person, public authority, agency or other body which, alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by union or member state law.

3.6

Data processors means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the data controller.

3.7

Processing means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination restriction, erasure or destruction.

3.8

Profiling means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to that natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

3.9

Pseudonymisation means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

3.10

Sensitive personal data includes information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition or sexual life, or about the commission of, or proceedings for, any offence committed or alleged to have been committed by that person, the disposal of such proceedings or the sentence of any court in such proceedings. Sensitive personal data may include biometric data and genetic data. Sensitive personal data can only be processed under strict conditions, and will usually require the express consent of the person concerned.

4. Data protection principles

4.1

We will comply with the data protection principles in Privacy Law. Under Privacy Law, personal data must be:

(a) Processed fairly, lawfully and in a transparent manner.

(b) Processed for specified, legitimate and specified purposes and not further processed in a manner that is incompatible with those

(c) Adequate, relevant and not limited to what is necessary for the purpose.

(d) Accurate and kept up to date. Personal data that is inaccurate will be erased or rectified without delay.

(e) Kept in a form that permits identification of the data subject for no longer than is necessary for the purpose.

(f) Processed in a manner which ensures appropriate security of personal data.

5. Fair, lawful and transparent processing

5.1

Privacy Law does not prevent the processing of personal data, but it ensures that it is done fairly and without adversely affecting the rights of the data subject. The data subject must be told who the data controller is, the purpose for which the data is to be processed by us, and the identities of anyone to whom the data may be disclosed or transferred. In dealing with suppliers, customers and other third party (excluding employees), typically we are acting as a data processor. We will inform you if we are to act as data controller.

5.2

For personal data to be processed lawfully under the applicable Privacy Law, certain conditions have to be met. These may include, among other things, requirements that the data subject has expressly consented to the processing, or that the processing is necessary for the legitimate interest of the data controller or the party to whom the data is disclosed. When sensitive personal data is being processed, more than one condition must be met. In most cases the data subject's explicit consent to the processing of such data will be required.

6. Collected for specific, explicit and legitimate purposes

6.1

We will only process personal data may for the specific purposes notified to the data subject when the data was first collected or for any other purposes specifically permitted by the applicable Privacy Law. This means that personal data will not be collected for one purpose and then used for another. Further processing for archiving in the public interest, scientific research or statistical purposes shall, in accordance with Privacy Law, not be considered incompatible with the initial purpose. If it becomes necessary for us to change the purpose for which the data is processed, we will inform the data subject of the new purpose before any processing occurs.

7. Adequate, relevant and non-excessive processing

7.1

We will only collect personal data to the extent that it is required for the specific purpose notified to the data subject. Any data that is not necessary for that purpose will not be collected.

8. Accurate data

8.1

Personal data must be adequate, relevant and limited to what is necessary for the specific purpose. Personal data must be accurate and kept up to date. If we identify information that is incorrect, misleading or is not accurate we shall take steps to check the accuracy of any personal data at the point of collection and at regular intervals afterwards. Inaccurate or out-of-date data will be destroyed. If you identify any data that we are holding which is incorrect, misleading or inaccurate, please advise us and we will take the necessary action to correct this.

9. Timely processing

9.1

Personal data will not be kept longer than is necessary for the purpose. This means that data will be destroyed or erased from our systems when it is no longer required. For guidance on how long certain data is likely to be kept before being destroyed, you can contact the Data Protection Compliance Manager.

10. Processing in line with data subject's rights

10.1

Data will be processed in line with data subjects' rights. Data subjects have rights to:

(a) Request access to data held about them;

(b) Prevent the processing of their data for direct-marketing purposes;

(c) Ask to have inaccurate data amended or deleted;

(d) Prevent processing that is likely to cause damage or distress to themselves or anyone else;

(e) Withdraw their consent to processing at any time;

(f) Request individual personal data in a portable form;

(g) Lodge a complaint with a supervisory authority;

(h) Request information regarding the existence of automated decision-making, including profiling (including meaningful information about the logic involved);

(i) Information regarding the retention period of personal data or, as a minimum, the criteria used to determine that period.

11. Records

11.1

We shall maintain a record of all categories of processing activities that we undertake including, the nature of processing and, where applicable and where permitted, details of transfers of personal data to a third party (sub-processors). If applicable under Privacy Law, we shall make such records available to a supervisory authority upon request.

12. Data Security

12.1

We will ensure that appropriate security measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data, including taking reasonable steps to ensure the reliability of our employees who may have access to personal data and will ensure that such employees are subject to appropriate confidentiality undertakings. Data subjects may apply to the courts for compensation if they have suffered damage from such a loss.

12.2

Security measure shall, amongst other things, include:
(a) the pseudonymisation and encryption of personal data;
(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
(c) the ability to restore the availability and access to personal data in a timely manner in the event of physical or technical incident;

(d) processes for regularly testing, assessing and evaluating the effectiveness of technical and organisations measures to ensure the security of the processing.

12.3

Details of our IT security measures are set out in our IT Security Policy.

13. Cooperation

13.1

We shall:
(a) provide reasonable cooperation to a data controller in relation to any individuals exercising their rights under Privacy Law, including but not limited to subject access requests;
(b) Save as where prohibited by law and as soon as reasonably practical, notify the data controller of any legal obligation which requires us to disclose personal data to a third party;
(c) Notify the data controller, not later than seventy-two (72) hours of becoming aware of it, of any personal data breach and provide reasonable assistance to the data controller with any investigation into and any remediation of the personal data breach;
(d) Notify the supervisory authority without undue delay after becoming aware of a personal data breach;
(e) Provide reasonable assistance with any notifications made to any relevant authorities and/or individuals in relation to a personal data breach and assistance to appropriate security measures are adhered to;
(f) Make available to the data controller all reasonable information to demonstrate compliance with the obligations set out in this policy.

14. Dealing with subject access requests

14.1

Any data subject may make a formal request for information that we hold about them in writing. We will not charge a fee for provision of this information, however, we may charge a nominal admin fee for further copies or access.

14.2

Data subjects have the right to receive personal data concerning him/her in a structured, commonly used and machine-readable format. In exercising his or her right to data portability the data subject shall have the right to have the personal data transmitted from one controller to another where technically feasible.

14.3

We will respond to written subject access requests within a reasonable period, but in any event no longer than thirty (30) days from the date of receipt.

14.4

All employees who receive a written request from a data subject will forward the request to the Data Protection Compliance Manager.

15. Providing information over the telephone

15.1

All employees dealing with telephone enquiries will be careful about disclosing any personal information held by us. In particular they will:

(a) Check the caller's identity to make sure that information is only given to a person who is entitled to it;

(b) Suggest that the caller put their request in writing if they are not sure about the caller's identity and where their identity cannot be checked;

(c) Refer to the Data Protection Compliance Manager for assistance in difficult situations. No one should be bullied into disclosing personal information.

16. Monitoring and review of the policy

16.1

This policy is reviewed annually by the Data Protection Compliance Manager.

16.2

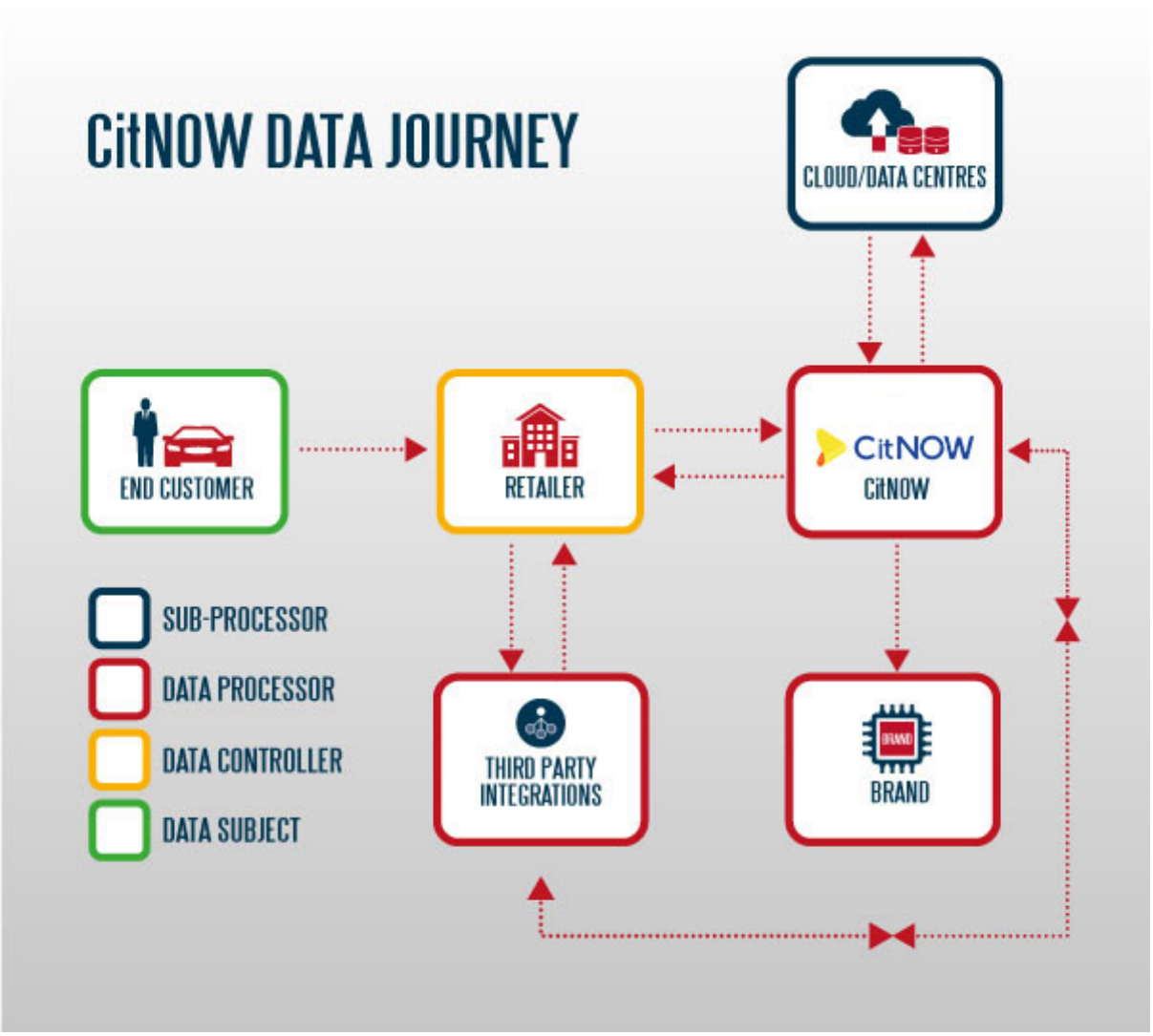
We will continue to review the effectiveness of this policy to ensure it is achieving its stated objectives.

17. CitNOW

17.1

In addition to our obligations set out in this policy, Our data protection position specifically relating to the provision of CitNOW is set out in our GDPR Statement for CitNOW Retailers below.

Zype TV Ltd - GDPR Statement for CitNOW Retailers



In providing CitNOW services to Retailers (Our customers) we are acting as a data processor and Our customer is the data controller, both as defined by Privacy Law. In this statement, as data controller Our customer is referred to as "You/Your" and CitNOW, as data processor is referred to as "We/Us/Our". We have outlined below Our responsibilities as the data processor and Your responsibilities as the data controller in providing CitNOW services to You and Your data subjects ("Consumers").

Part A – Our Responsibilities

1. General

1.1 Type of Data and Use

The type of data that we gather and process in providing the CitNOW service to You and Your Consumers includes:

- Videos of Your Consumer's cars, which may show the registration number
- Contact details for Your Consumers, which may include email addresses and telephone numbers
- Videos of members of Your staff
- Videos of Your Consumers

As a point of clarity, the data that we use in the CitNOW service may constitute personal data as defined by Privacy Law, but is not deemed sensitive personal data.

1.2 Data Security

It is Our responsibility to ensure Your data is kept safe and we have a comprehensive IT and Security Policy which details what measures we take to ensure the security of the data.

In summary, all the data we process is held on secure servers. Any data originating in the EEA is stored on servers located in the EEA and is not transferred outside of the EEA without the data controllers prior written consent.

We utilise third party servers to store data and such third parties act as sub-processors of the data. We have selected reputable sub-processors to provide, amongst other things, data storage, quality checking and analytics. They are contractually bound to abide by the principles of Privacy Law and we are satisfied that they have adequate security systems in place to protect Your data. Our sub-processors are also bound to ensure any third parties services they employ are bound by the same conditions with regards to data security as we have agreed with them.

We shall maintain an up to date list detailing the location of all personal data together with details of any third party sub-contractor or third parties to whom we have shared any personal data. If You are unhappy with any sub-processor that we do or intend to use, You have the right to object to us using such sub-processor. We will discuss with You appropriate options in such event.

We shall be responsible for the acts and omissions of Our sub-processors as if they were the acts and omissions of us (as data processor).

1.3 Data Transfer

Our sub-processors may not transfer data outside of the EEA without Our permission.

For data from countries located outside of the EEA we utilise servers located in the EEA for data storage, but also may store some data on local servers where appropriate.

If You are a customer located outside the EEA, we require You, to notify us of any local data protection regulations in a jurisdiction outside of the EEA with which we need to comply.

In the event that there are any changes to Our data storage that involves transferring data outside of the EEA We will notify You of this in advance for Your approval as data controller. We will also employ the use of the EU Model Contract Clauses, or similar, where necessary for such data transfer.

1.4 Online Services

We have defined Our Online Services (Our dashboard and reports) in Our factsheet.

We only grant access to Our Online Services to Your employees and representatives that You notify to Us ("Authorised Users"), including the setup of a "manager" role for at least one of Your Authorised Users. Once access to CitNOW is granted to a Manager, the Manager will be responsible for actioning the addition and deletion of any further users requiring access to CitNOW. All Authorised Users and Managers will receive training on the use of the CitNOW dashboard.

Data is also shared with brand owners and vehicle manufacturers via Our Online Services. This includes information regarding Your use of the CitNOW service as well as personal data we may collect as part of the CitNOW service. Brands are required to nominate Authorised Users to access the Online Services. We have appropriate arrangements in place with brand owners and vehicle manufacturers to ensure their compliance with applicable Privacy Laws and to prevent them from processing any personal data which they may see via Our Online Services for any reason other than reporting and analytics.

We may also use Your videos for the purpose of demonstrating the CitNOW service i) within Your dealer group and ii) with the vehicle manufacturer. You agree that we may use such materials for this purpose.

1.5 Storage

CitNOW is not intended for the long-term storage and archiving of Your Content. Our policy in respect of management and deletion of Your Content is as follows:

(a) Online Services content will not be accessible by You following termination;

(b) Upon termination: (i) subject to payment of the applicable fee and at your request we will provide you with a copy of the Content you have uploaded to the Online Service and/or (ii) Content may be moved to hosted storage;

(c) At any point following termination, You may provide us with a written request to retrieve and supply you with a copy of specified Content;

(d) Subject to Our compliance with Section 14 of this Data Protection Policy, We reserve the right to charge a reasonable administrative fee for Content retrieval and will seek Your acceptance of any administrative fee prior to undertaking Content retrieval;
(e) Whilst CitNOW will consider all requests for Content retrieval, we cannot guarantee successful retrieval of Content following termination.

1.6 Communications to Consumers

CitNOW will not market directly to Consumers unless We receive an express instruction from You for a specific purpose and confirmation from You that necessary consents have been sought. Should a Consumer wish to exercise their right to be forgotten, We will facilitate such request.

Part B – Your Responsibilities Under GDPR

2. General

The type of data that we gather and process in providing the CitNOW service to You and Your Consumers includes:

2.1 Consent

You are responsible for informing Your Consumers of the type of and nature of the personal data that You gather from them and for gaining their consent as to how this is used, stored and accessed within Your organisation. This includes the use of personal data in the CitNOW Service as part of the overall communication strategy and the general operational running of Your business. Examples of the personal data gathered and used as part of the CitNOW service would be:

(a) When a video is sent from the service department as part of a service: In this scenario personal data is required in order to process their car for a service;

(b) When a video is sent from the sales department as a result of an enquiry: In this scenario, personal data is gathered in order to respond to the customer with details of a vehicle they are interested in purchasing.

Examples of personal data used in these circumstances are:

- telephone number
- email address
- home address
- car registration

Consumers should be made aware that the specific examples above are necessary for the day to day operational running of Your business and that their personal data is used for this purpose. It is Your responsibility to ensure that you have a clear policy for data use and data retention once You have used personal data for its original purpose. You should be aware that unsolicited videos – for example, sending a Consumer a video to promote a new car offer when they have not specifically asked for it – would count as marketing under GDPR regulations and in this scenario, the Consumer should have given their express consent to such communication.

You are also responsible for advising Your staff that the use of their personal data in the CitNOW service is part of the general operational running of Your business and for gaining their consent to such use in the appropriate employment agreements with them.

2.2 Security

You are responsible for controlling access to any personal data collected by the CitNOW services and for ensuring each individual working within Your organisation and having access to personal information is aware of, and complies with, their obligations under the applicable Privacy Law and this policy. User names and passwords must not be shared.

2.3 Warranty

You acknowledge the nature of the service we deliver and You warrant that You have sought the necessary consents set out in section 2.1 above and give us permission and authority to gather, store and share Your data in line with this statement.