AUTOPROTECT HELLAS LTD

Confidentiality and Data Protection Policy 2018 v.2

1. Aims and Objectives

1.1. This policy is set out to identify how

NGN Autoprotect Hellas Ltd (APH)

executes its duty to keep personal information safe and confidential whilst at the same time, not compromising its ability to share information where it is needed.

1.2. The purpose of this Confidentiality Policy is to lay down the principles that must be observed by all who work within the organisation including outsourced or temporary personnel and have access to personal information.

1.3. APH is committed to maintaining the confidentiality of personal information that it handles. Any information given or received in confidence for one purpose will not be used for another purpose, or passed to a third party, without their consent except in special circumstances e.g. to prevent harm to an individual.

1.4. APH will ensure that personal information is obtained, used and disclosed in accordance with the common law duty of confidentiality and the Data Protection Law 2472/97.

1.5. APH will also have full regard for current and future legal requirements which impinge on the confidentiality of:

1.5.1. Personal information in general, and

1.5.2. Specific categories of personal information e.g. Traffic Violations of insureds.

2. Principles

In accordance with the Principles of the Data Protection Law, personal information held in both computerised and manually filed records will: -

2.1. Be obtained and processed fairly and lawfully,

2.2. Be used only for the specified purposes for which it was obtained and not in any manner incompatible with those purposes,

2.3. Be adequate, relevant and not excessive for those purposes,

2.4. Be kept accurate and where necessary up to date,

2.5. Not be kept longer than is necessary for those purposes,

2.6. Be processed in accordance with individuals' rights under the Law,

2.7. Be protected from unauthorised access, unlawful processing, accidental loss, destruction or damage,

2.8. Not be transferred to a country which does not ensure adequate protection for the rights of individuals in relation to the processing of personal information.

3. Definitions

3.1. 'Confidentiality' applies to information whether received through formal channels (e.g. in a formal accident report), informally, or discovered by accident.

It applies to organisational business, employees and potential employees, temporary staff, clients, individuals, or organisations who come into contact with the company i.e. external contractors /partners.

3.2. Information which can be classified as 'Confidential', can broadly be grouped into the following areas: -

3.2.1. Information of a specific and personal nature about Insureds / Beneficiaries, employees or partners. If this type of information is used inappropriately, it can cause individuals to face discrimination, harassment or harmful actions and inappropriate decisions by others.

3.2.2. Sensitive organisational information. This may be used to damage the company and other organisations, as well as individuals and staff. It may be prejudicial to the business of the company or used to threaten the security of its property and systems.

3.3. Breaches in confidentiality happen when sensitive information is given to people who are not authorised to access it. They are most likely to happen when procedures have not been agreed or followed. They can also happen when information is passed between sections, departments or organisations, or when information is being stored insecurely.

4. Informed Consent

4.1. Where it is proposed, in exceptional circumstances, that information about an individual should be shared with another organisation or company, the consent of the individual, or the person who provided the information, should normally be sought.

4.2. This should be done in such a way that those persons know exactly what information will be passed on, to whom and for what purpose.

4.3. Information which is confidential and restricted will only be passed on where there is a clear need to know and where the expressed and informed consent has been obtained from the person whose information needs to be passed on.

4.4. Wherever possible informed consent should be recorded in writing as a form of contract which gives the agreed terms and conditions of passing on and storing this information.

4.5. Informed consent should be sought every time there is a need for confidential information to be passed on to an unauthorised person.

4.6. Confidential information will not be discussed on the telephone unless the identity of the caller is established, this will be checked when necessary, e.g. with call-backs and/or security checks prior to the release of any information.

4.7. Refusal to give consent should be respected wherever possible.

5. Employee Responsibilities

5.1. In normal circumstances, staff may only disclose personal information outside the organisation if one or more of the following applies:

5.1.1. The disclosure is routinely necessary for the purpose for which the information is held and the individuals about whom the data is held have been made aware of, or could reasonably expect, such a disclosure to be made;

5.1.2. The disclosure is a legal requirement under the legislation governing the operation of the service or function concerned;

5.1.3. The receiving staff member 'needs to know' the information in order to carry out their duties;

5.1.4. The person about whom the information is held has given valid consent to the disclosure

5.2. Where it is not possible to obtain valid consent, information may exceptionally be passed on when there is a legal basis for overriding the usual non-disclosure e.g.

5.2.1. The disclosure is required under direction of a Court Order, or in the course of law enforcement, e.g. In cases of co-operation with the police in relation to an accident or a crime committed involving an insured vehicle;

5.2.2. The disclosure is provided for agreed inter-company procedures which have a legal basis for their operation, e.g. Underwriting procedures for the assessment and management of high risk individuals or risks insured;

5.2.3. Where this is an overriding public interest in disclosing the information such as evidence of a risk of serious harm to the individual or in order to prevent or detect a serious crime.

5.3. When passing information to others, staff should:

5.3.1. Check that the source of the request is bona fide;

5.3.2. Ensure that the recipients understand and accept their obligation to respect the confidentiality of the information;

5.3.3. Only send the information necessary for the purpose of the disclosure;

5.3.4. Record exactly what has been passed on, to whom, when and why.

5.4. When receiving information from others, staff should:

5.4.1. Ensure that any information received in confidence should be marked as such to ensure it is not inadvertently disclosed to third parties;

5.4.2. Ensure that only information necessary for the purpose of the service performed should be requested.

5.4.3. Ensure that information requests include a confidentiality statement.

5.5. All staff employment job descriptions and temporary staff role descriptions must contain a statement enforcing the duty to respect the confidentiality of information.

5.6. Staff, outsourced partners, temporary staff and volunteers will be asked to sign declarations of confidentiality on commencing employment / cooperation with APH either as part of their staff contract or as a separate statement.

5.7. All employees and temporary staff are responsible for:

5.7.1. Checking that any personal data that they provide to APH is accurate and up to date.

5.7.2. Informing APH of any changes to information which they have provided, e.g. changes of address.

5.8. Sensitive information is only to be requested on a 'need to know' basis. This means only when the information is necessary to provide a service or to manage a case file or support effectively, and then only in the best interest of beneficiary.

6. Compliance

6.1. APH will ensure that staff, temporary staff and outsourced partners receive adequate training and guidance on their duties and responsibilities in relation to the handling, disclosure and storage of personal information.

6.2. Managers must ensure that everyone concerned are made aware of the limits of their responsibilities, and where they may seek advice, should they have an information request which falls outside their responsibilities.

6.3. In accordance with the company's disciplinary procedures, disciplinary action will be taken against any member of staff who fails to carry out the duties and responsibilities set out in this Policy or the procedures which follow from it.

6.4. Where contractors are used, the contracts between APH and these third parties will contain clauses to ensure that contract staff are bound by the same code of confidentiality as employed staff.

6.5. This policy has been approved by the Board of Directors and any breach will be taken seriously and may result in formal action. Any employee who considers that the policy has not been followed in respect of personal data about themselves should raise the matter with their dept manager or the Data Controller in the first instance.

7. The APH's Designated Data Controller

APH is responsible for ensuring compliance with the Data Protection Law and implementation of this policy on behalf of the Managing Director. The Data Controller is Mr. Nikitas Koutsourais who is registered with the dpa (www.dpa.gr), e-mail: nkoutsourais@autoprotect.gr. Any questions or concerns about the interpretation or operation of this policy should be taken up in the first instance with the Data Controller.

8. Data Security

8.1. The need to ensure that data is kept securely means that precautions must be taken against physical loss or damage, and that both access and disclosure must be restricted. All staff are responsible for ensuring that:

8.1.1. Any personal data which they hold is kept securely

8.1.2. Personal information is not disclosed either orally, in writing or otherwise to any unauthorised third party.

8.2. Documents containing individual data must not be left visible where it can be read by anyone inappropriately. This includes telephone messages, computer prints, letters and other documents.

8.3. Desks must be cleared each evening and electronic documents closed down when leaving a desk.

8.4. All hardware containing data must be housed in a secure environment.

8.5. Personal data must not be stored on the hard disc of a laptop or flash drive unless it has been encrypted. (For further information on that please ask Mr. Nikos Iliopoulos - IT Controller)

8.6. All media containing staff information must be destroyed in a manner that ensures that data is not disclosed to an unauthorised person. Manual records should be shredded before disposal.

9. Rights to Access Information

9.1. In accordance with individuals' rights of access under the Data Protection Law, APH will, on request, inform an individual whether or not information is kept about them and, if so, will provide a copy of that information. Any person who wishes to exercise this right should make the request in writing to the Data Controller.

9.2. APH aims to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within 5 days of receipt of a written request unless there is good reason for delay. In such cases, the reason for delay will be explained in writing to the individual making the request.

9.3. All individuals who are the subject of personal data held by APH are entitled to:

9.3.1. Ask what information the company holds about them and why.

9.3.2. Ask how to gain access to it.

9.3.3. Be informed how to keep it up to date.

9.3.4. Be informed what the organisation is doing to comply with its obligations under the Data Protection Law 2472/97.

10. Publication of APH Information

Information that is already in the public domain is exempt from the Data Protection Law. This would include, for example, information on insurance partners contained within externally circulated publications. Any individual or organisation that has good reason for wishing details to remain confidential should contact the Data Controller.

11. Retention of Data

11.1. APH will keep information as per its legal obligations (i.e. physical 5 years / electronic 15 years). All staff are responsible for ensuring that information is not kept for longer than necessary.

11.2. The purpose for holding personal data and a general description of the categories of people and organisations to whom we may disclose it are listed in the Data Protection register. This information may be inspected or obtained from the Data Controller.
