Insurance Ireland Guidance on Data Protection Requirements for Insurers When Handling Personal Data (January 2024)

Introduction

Data Protection is the means by which the privacy rights of individuals are safeguarded in relation to the processing of their personal data. The General Data Protection Regulation (the "Regulation") and the Data Protection Acts 1988 to 2018 (the "Data Protection Acts") confer rights on individuals as well as placing responsibilities on persons processing personal data.

This "*Guidance on Data Protection Requirement for Insurers When Handling Personal Data*" has been prepared by Insurance Ireland in consultation with the Data Protection Commission ("DPC"). The Guidance is intended to assist insurers in Ireland in meeting the requirements of the Regulation and the Data Protection Acts and sets out how they might comply with the legislation when collecting, handling and storing personal data.

This guidance may also be useful for consumers in understanding what personal data may be collected by insurers, how such data may be processed and the rights that may be available to them.

Scope

This Guidance considers the seven principles of data protection, obligation of data controllers and rights introduced under the Regulation as they apply to Irish insurers.

The information contained in this document is for information purposes only and is not legal advice. Specific legal advice should always be sought on the application of the law in any particular situation.

Table of Contents:

Table of Contents:

Section A: Key Principles of processing personal data

Articles 5 (1) and (2) of the Regulation sets out key principles of processing personal data.

The seven data protection principles require that personal data must be:

1. Processed in a lawful, fair and transparent manner ('lawfulness, fairness and transparency');
2. Collected for specified, explicit and legitimate purpose and not further processed in a manner that is incompatible with those purposes ('purpose limitation');
3. Adequate, relevant and limited to what is necessary ('data minimisation');
4. Accurate and where necessary, kept up-to-date ('accuracy');
5. Kept in a form which permits identification of data subjects for no longer than is necessary ('storage limitation')
6. Processed in a manner that ensures appropriate security of the personal data ('integrity and confidentiality'); and
7. Processed in a way that allows data controllers to be able to demonstrate compliance with the principles (accountability).

1. Lawfulness, fairness and transparency

Insurers collect personal data from application forms, claim forms and other documentation completed or provided by the individual as well as through call centres, meetings with individuals and digital channels e.g. by point of sale systems or over the internet. Personal data may be kept on computer systems and/or in paper files. The detail regarding the collection and processing of personal data is contained in the Privacy Notices of the individual insurers, which are made available to data subjects.

While most personal data is collected directly from the data subject, insurers also obtain personal data via third parties, for example from agents, brokers, solicitors, trustees, employers, licensed private investigators, health professionals, social media and other insurers.

1.1 Collection

Personal data will be collected by insurers in accordance with a lawful basis provided for in the Regulation. The majority of data processing may be carried out where it is necessary for the performance of the contract of insurance or where it is necessary for compliance with a legal obligation, as regulated financial services providers. Other processing is carried out with the consent of the data subject, where necessary for legitimate interest purposes and where proportionate. However it should be noted that other lawful bases are provided for in the Regulation (See section 2.1 of this Guidance).

The collection of data by insurers happens at three main stages:

A. At application or proposal stage:

In order to assess the risk, determine the premium, including any special provisions and to comply with the relevant identification and other legislative requirements such as the Criminal Justice (Money Laundering and Terrorist Financing) legislation in addition to the Central Bank of Ireland's Consumer Protection Code, insurers request appropriate and relevant information. This information should be limited to meet the specific provisions of the legislative requirements and, depending on the particular product or service, can include (but not limited to):

- Personal details (such as name and date of birth);
- Contact details;
- Information about the applicant's health;
- Payment information;
- Information regarding financial situation and goals;
- Driving history;
- Claims experience;
- Other information to comply with specific legislative requirements.

B. During the term of the policy:

For the administration of a policy by the insurer, certain additional information may be required, including information collected at renewal and for payment of premiums while the policy is in force. Updates to information such as contact details and information may be required under new regulations and law (for example, tax information).

C. When claims are made:

An insurer may again require detailed health and other relevant and appropriate information in order to assess whether a claim is payable under the policy, and if so, what amount should be paid. Recognising that circumstances can differ between claims, only data specific to the purpose of assessing the validity of a claim, or to assess non-disclosure relevant to the claim or the policy, should be requested in order to determine liability and compensation level.

The lawful bases supporting the collection and use of personal data during the above three stages are contractual performance, legal obligation and processing necessary to establish, exercise or defend legal claims.

1.2 Information

To comply with the principle of lawfulness, fairness and transparency insurers should:

- where customer personal data is collected, provide access to a privacy policy containing information about how and why the personal data is collected and used. Privacy Notices should contain the information required under Article 13 and/or Article 14 of the Regulation and the advice contained in the Article 29 Working Party's (now the European Data Protection Board (EDPB)) Guidelines on Transparency, which can be found here;
- at a suitable point in the business process, make an appropriate privacy notice available to third party claimants who would not otherwise have received the information, for example when responding to the claimant's initial communication;
- where other information sources are used to independently verify information provided by the insured (e.g. industry databases of claims information), ensure that details of the existence and purpose of each means of verification which could be used is included in the relevant Privacy Notice or customer documentation. Where the Insurance Link database is to be accessed for general insurance as part of the underwriting process, the customer must be made aware of this at point of sale, prior to underwriting and through the Privacy Notice;
- ensure that any named driver is made aware of the details of the Privacy Notice which has been provided to the motor insurance customer;
- ensure that data subjects are advised that telephone conversations (whether inbound or outbound) are recorded, where this is the case, and the purposes of the recordings, including if the recording is used for any purpose other than processing of

the policy. It is recommended that firms have a procedure in place if the data subject objects to the recording documenting what the process is in this instance. It should be noted that if the customer is purchasing an insurance policy via telephone, the customer will receive a copy of the information shared in order to meet requirements under applicable distance selling and consumer protection laws.
- where relevant make it clear to customers and claimants that personal information may be sought from other insurance companies who hold a policy or other relevant information about a risk;
- in respect of non-life insurance policies, only require the provision of personal data relating to potential claimants in accordance with Appendix 4; and
- where relevant, highlight in the Privacy Notice or customer documentation that a private investigator may be instructed by an insurer to investigate a claim (see Appendix 2).

1.3 Personal data shared with other entities

It is important to note insurers may also share personal data with other entities, including:

- persons acting on the customer's behalf e.g. insurance intermediaries, loss assessors, solicitors, executors, etc;
- the Financial Services and Pensions Ombudsman, the Central Bank of Ireland or any equivalent foreign supervisory or complaints body;
- other group companies (depending on purpose, and subject to disclosure of this fact to the customer);
- other insurance companies, where this is clearly stated on the application or claim form, Privacy Notice or other correspondence with a claimant. In the unlikely event of a mismatch occurring which results in the accidental disclosure of information to another insurer, the information will be destroyed immediately upon receipt, once this issue is identified;
- Insurance Ireland, or its agents, which administer several industry databases on behalf of its member companies e.g. Insurance Link (see Appendix 3);
- the Motor Insurers' Bureau of Ireland;
- An Garda Síochána, the Revenue Commissioners or any other person authorised by law to access customer records. Such requests should be in writing to the insurer and quoting the legal basis for seeking access to the personal information;
- agents of the insurer e.g. loss adjusters and other external investigators, medical practitioners, solicitors, firms responsible for computer maintenance or similar services, other subcontractors or advisers;
- reinsurers, where the insurance risks associated with a contract of insurance is reinsured; and
- other bodies with regulatory or statutory powers including the Data Protection Commission, the Pensions Authority etc.

2. Legitimate Purposes

Principle 2, purpose limitation as set outlined in Article 5 (1) (b) of the Regulation, requires that personal data shall be "*collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes*".

There are two parts to this rule. Firstly, personal data must be processed in accordance with a legitimate and specific legal basis which is clearly set out prior to data collection, and secondly, that processing must only take place in ways compatible with the purposes for which it was provided or purposes compatible with the original purposes.

2.1 Processing in accordance with legitimate and specific purposes

In practice this means that insurers are only permitted to keep personal data in accordance with a legitimate and specific legal basis which is clearly stated at the outset. Insurers process personal data in accordance with at least one of the grounds listed in Article 6 of the Regulation which include:

(a) processing is necessary for the **performance of a contract** to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
(b) processing is necessary for **compliance with a legal obligation** to which the controller is subject;
(c) processing is necessary in order to **protect the vital interests** of the data subject or of another natural person;
(d) processing is necessary for the establishment, exercise or **defence of legal claims;**
(e) 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 controller;
(f) processing is necessary for the purposes of the **legitimate interests** pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child; or
(g) the data subject has given consent to the processing of his or her personal data for one or more specific purposes.

The processing of special category data is prohibited under Article 9(1) of the Regulation unless it falls within certain conditions as set out in Article 9(2) of the Regulation and in the Data Protection Act 2018. Conditions include that the data subject has given explicit consent to the processing of those personal data for one or more specified purposes and; processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent. At least one of these conditions set out in Article 9(2) is required in addition to a legal basis in Article 6.

In addition, section 50 of the Data Protection Act 2018 provides that subject to, suitable and specific measures being taken to safeguard the fundamental rights and freedoms of data subjects, the processing of data concerning health shall be lawful where it is necessary and proportionate for a number of activities, including:

- a policy of insurance or life assurance;
- a policy of health insurance; and
- an occupational pension, a retirement annuity contract or any other pension arrangement;

The suitable and specific measures used by insurers include, but are not limited to - purpose limitation, restricted access, training for those involved in the processing and confidentiality requirements for staff handling medical data.

Under Article 10 of the Regulation, the processing of data relating to criminal convictions and offences is also prohibited. However, under section 55 of the Data Protection Act 2018, there are a number of exemptions from this restriction. At least one of these exemptions is required in addition to a legal basis in Article 6 when processing data relating to offences or convictions.

Primary acceptable uses of personal information by insurers include the following:

- where relevant, personal information is used to advise on or determine suitability of insurance products;
- to provide quotes;
- to underwrite the risk proposed;
- to administer the policy;
- to assess and process any claims arising under the policy;
- to comply with applicable legal requirements;
- to participate in internal or market-level statistical exercises; and
- to handle complaints.

A secondary purpose/use of personal information by insurers is direct marketing of products to existing and potential customers. Direct marketing activity requires an appropriate level of consent from the customer under Regulation 13 of the ePrivacy Regulations (SI 336 of 2011).

Any further proposed processing should be assessed to check whether it is compatible with the original purposes and, where it is not, the new purpose should be brought to the attention of the data subject along with all information about the new purpose required under Article 13 and/or Article 14 of the Regulation prior to carrying out that further processing.

2.2 Use and disclose it only in ways compatible with the purposes for which it was originally obtained

Insurers must ensure that any use or disclosure of personal data must be necessary for or compatible with the purposes for which the data is collected or otherwise in compliance with Data Protection legislation.

Any further proposed processing should be assessed to check whether it is compatible with original purposes. If a new processing activity is proposed that does not fall within a purpose previously notified to data subjects, a further notification will usually be required prior to the processing activity beginning.

Furthermore, consent (or explicit consent) may need to be obtained from the data subjects depending on the lawful basis that was originally relied upon.

3. Data Minimisation

To comply with the principle of data minimisation, insurers must:

1. Not collect any more personal information than is necessary for the purposes explained in section 2 above; and
2. Check the types and sources of information being collected from customers on an ongoing basis to ensure that only relevant information is sought and collected.

Insurers must comply with all other relevant statutory obligations, e.g. duties under the Equal Status Act 2000 – 2018 to use only underwriting criteria which can be justified on commercial or actuarial grounds.

For certain types of life assurance policies, particularly in relation to critical illness cover, an insurer may request information about a proposer's family medical history. Questions should be prescriptive and specific as to the family illnesses and not open ended. This information may be used only in underwriting the proposer's application and may not be used in

underwriting the application of any third party who is related to the applicant. Appropriate access restriction procedures must be in place to ensure that this practice is followed.

From time to time, insurers request medical information directly from medical practitioners as part of their claims processing procedures. Any requests for medical information should be focused and not excessive and only data specific to the purpose of assessing the validity of a claim, or to assess non-disclosure relevant to the claim should be requested in order to determine liability and compensation level.

Under Data Protection legislation, the provision of explicit consent by an individual for the release of information permits the Data Controller, e.g. an individual's GP, treating hospital or dentist, to give consideration to releasing the requested information as long as it is not excessive. In this regard, general requests by insurers to medical practitioners for full medical files, even with the consent of the individual, would not generally be acceptable.

PPS Number data may be collected by insurers where required by legislation. Use of this information will be restricted to the specified use required by law and the specific reason this is required should be disclosed.

4. Accuracy

The insurer shall ensure that data is kept accurate, complete and up to date in accordance with the Regulation and the Data Protection Acts.

In accordance with the principle of accuracy, the following principles should be observed:

- the insurer shall have appropriate procedures in place to check the accuracy of information when it has been entered on the insurer's systems. For example, providing customers with a detailed summary of the policy information and asking them to review and correct any inaccuracies;
- the insurer shall have appropriate procedures in place that allow data subjects to inform the insurer of incorrect personal data. Updating personal data such as an address change, new payment details or a change of name is not considered a correction of personal data (because the original data was accurate when collected and it may be necessary to retain the previous details for normal record keeping purposes) and will therefore be handled in line with normal policy servicing procedures; and
- where inaccurate personal data is otherwise identified, the insurer should correct it in line with the Regulation and the Data Protection Acts.

5. Storage limitation

The principle of storage limitation sets out that personal data shall be 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. To comply with this principle, insurers must have a written data retention policy. Insurers must also adhere to and include in their written data retention policy the retention periods and retention guidance.

It should be noted that there are a number of legislative and regulatory obligations which require insurers to retain personal data to demonstrate compliance with these rules. For example, policyholder information may be held for a period of at least 6 years after the ending of the client/insurer relationship to take account of the insurer's responsibilities under the Statute of Limitations, the Central Bank Consumer Protection Code and relevant

provisions of the Criminal Justice (Money Laundering and Terrorist Financing) legislation. Limited policyholder information may be held, in narrow circumstances, for longer periods by insurance companies to allow for compliance with other legislation requiring such information (e.g. Unclaimed Life Assurance Policies Act, health insurance legislation and lifetime community ratings legislation). In certain cases, information may be retained for longer periods where it may be required for the investigation of claims.

Where an Insurer provides a quotation, but the policy was not subsequently incepted and the customer opted to receive direct marketing during the quotation process, the information provided may be used to direct market the customer the following year. The customer can be contacted again in subsequent years as long as they are given the opportunity to opt out at each contact and have not taken up this opportunity.

Where a policy quote is not proceeded, there are a number of reasons why insurers may have to retain certain data about the applicant, including the need to demonstrate fair treatment to regulators, in event of complaints to the Financial Services & Pensions Ombudsman (FSPO) and for fraud prevention purposes. Where an individual proposes for, but does not subsequently proceed with, a life assurance policy, or is declined, underwriting details may be kept on file in line with Consumer Protection Code requirements to facilitate a subsequent application or as a check against non-disclosure, or to evidence compliance with appropriate regulations in the underwriting process.

Overall, insurers must each assess the type of data that is retained, the period of time for which it is agreed to retain the data and clearly document the rationale for this assessment.

Changes to InsuranceLink's operations and processes (including data retention policies) are managed by the InsuranceLink Oversight Committee (ILOC), which acts independently of the Board of Insurance Ireland. ILOC was established as part of a set of binding Commitments offered to the European Commission by Insurance Ireland and finalised on 30 June 2022 pursuant to Article 9 of Council Regulation (EC) No 1/2003.[1]

6. Security

To comply with the principle of integrity and confidentiality set out in Article 5 of the Regulation, insurers must ensure that appropriate technical and organisational measures are taken against security risks, and that measures are in place and impact assessments are performed where required.

Good practice ensures that:

- Measures are in place to protect against unauthorised access to, or alteration, disclosure or destruction of the data and against their accidental loss or destruction;
- Appropriate procedures are in place in relation to back-up of data;
- Particular focus is placed on the security of personal data held on portable devices, with appropriate security measures such as encryption applied;
- Robust procedures are in place for limiting access to personal data and that staff are aware of these limits;
- An appropriate external access procedure is in place to ensure that only the data subject or their clearly appointed/authorised representative has access to their personal data. Examples of appointed/authorised representatives could include servicing agents, tax advisers, solicitors or an attorney under a Power of Attorney;

[1] https://insurancelink.insuranceireland.eu/wp-content/uploads/2022/07/C_20224.pdf

- Measures are in place pertaining to the collection, processing, keeping and use of medical information, other special category data and criminal offence data;
- Access to all special category and criminal offence data is restricted to authorised staff only. In particular it is expected that access to medical information should be restricted to relevant underwriters, claims assessors and persons needing to access a particular file as part of their role (e.g. members of staff dealing with data protection rights, such as Data Access Requests); and
- An appropriate personal data breach policy is in place which adheres to the rules set out in Articles 33 and 34 of the Regulation.

Insurers should also consider other data security measures such as logging mechanisms to permit verification of whether and by whom the personal data have been consulted, altered, disclosed or erased, pseudonymisation and/or encryption of the personal data.

7. Accountability

Insurers will ensure that appropriate technical and organisational measures are taken to be able to demonstrate compliance with the principles as set out in the Data Protection Acts and the Regulation, including the implementation of policies and procedures and the carrying out of impact assessments where required. Of particular importance are Articles 30, 35, 24 and Article 5 (2) of the Regulation.

Section B: Obligations on insurers introduced by the Regulation

In addition to adhering to the principles outlined above, in their role as data controller insurers are subject to further obligations introduced by the Regulation. These include the following:

1. Appointment of Data Protection Officer

As the processing of personal data is central to the business model of the insurance industry, each insurer must designate a Data Protection Officer (DPO) in line with Article 37, 38 and 39 of the Regulation.

As set out in the Regulation, the role of the DPO includes:

- Informing and advising the insurer as to its obligations either as a controller or a processor;
- monitoring compliance with the Regulation; and
- being the point of contact for both the Data Protection Commission (DPC) and data subjects with regard to issues relating to the processing of personal data, including the exercise of rights.

In addition to this the DPO must be involved in all issues relating to the protection of personal data.

The DPO will be easily accessible as a point of contact for employees, customers and the DPC. Customers will be advised of contact details of DPO should they have any queries relating to their personal data.

For further guidance on the role of the DPO please see Article 29 Working Party (now the European Data Protection Board (EDPB)) guidelines, available here.

2. Data Protection Impact Assessment (DPIA)

A DPIA is the process of systematically considering the potential impact that a processing operation may have on the privacy rights and freedoms of data subjects. This requirement allows insurers to identify potential privacy issues before they arise and put in place suitable mitigation measures.

In line with Article 35 and 36 of the Regulation, if processing is likely to result in a high risk to the rights and freedoms of natural persons, insurers must conduct an assessment of the impact of the envisaged processing operations on the protection of personal data. This is particularly applicable where the processing involves new technologies. While it is up to each insurer to define what is high risk, the DPC sets out a number of scenarios that would be considered 'high risk' for data processing purposes in its guidance.

Where a DPIA indicates that the risks identified cannot be mitigated the insurer must consult with the Data Protection Commission prior to commencing the processing in question.

3. Data Protection by design and default

Article 25 of the Regulation sets out that data protection by design and data protection by default are fundamental principles of future planning.

Data protection by design means that insurers will embed data privacy features and data privacy enhancing technologies directly into the design of their projects at an early stage as appropriate to the risk to the rights and freedoms of the data subjects.

Data protection by default means that the user service settings (for example no automatic opt in) on customer account pages, must be automatically data protection friendly, and that only data which is necessary for each specific purpose of the processing should be gathered at all.

4. Data breaches assessment and reporting

A 'personal data breach' is defined in the Regulation as "*a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed*".

In accordance with Article 33 of the Regulation, when a personal data breach has occurred, the insurer is obliged to report the incident to the Data Protection Commission within 72 hours if the breach is deemed to result in a risk to the rights and freedoms of data subjects. The DPC has published a Practical Guide to Personal Data Breach Notifications which is available here and the European Data Protection Board has published useful guidelines on examples regarding personal data breach notification which are available here.

There is an obligation on the insurer to have systems in place to detect incidents which might give rise to a personal data breach and to carry out an assessment of whether or not that breach is likely to result in a risk to the rights and freedoms of data subjects. Following detection of breach incidents insurers will assess the potential severity of the impact the breach may have on affected persons and act accordingly.

Once the breach has been identified as likely to result in a risk to the rights and freedoms of natural persons, the insurer will need to notify the DPC. If the breach is deemed to pose a high risk to the affected individuals, then the insurer will need to notify the data subjects. The breach notification forms are published on the Data Protection Commission's website.

It is important to note that even where an assessment indicates that a breach is unlikely to result in such a risk, there remains a requirement to keep a record of the incident in an internal register of breaches (Article 33(5) of the Regulation).

Section C: Rights of Data Subjects

The right to be informed

Under Articles 13 and 14 of the Regulation, all controllers must provide certain information to data subjects at the time when their personal data is collected. The document setting out this information is usually called a Data Protection Notice, Privacy Notice or similar and can be found on the insurance company's website and relevant application forms.

Such notices must include relevant contact details, why the information is being processed and the legal basis for the processing, how long the information is kept for, to whom it may be disclosed and the rights of the data subjects. The information must be provided in a form which is easily accessible, in clear and plain language and free of charge.

For further guidance on the information requirements under the Regulation, please see the European Data Protection Board's guidelines on compliance with the transparency requirement under the Regulation (including the Articles 13 and 14 requirements), which can be found here.

The right to access information

In accordance with Article 15 of the Regulation every Data Subject has the right to request access to personal information that the insurer holds about them. In response the Data Controller must provide all the information without undue delay or, at the latest, within one month of receipt of the request. (In limited circumstances where accessing the information is complex or where there is a high volume of requests, this period can be extended by a maximum of a further two months). The purpose of an access request is to make a data subject aware of and allow them to verify the lawfulness of processing of their personal data.

In addition to this personal information, the data subject is also entitled to the following information:

1. Purpose of the processing
2. Categories of data processed
3. Recipients or categories of recipient's data (note that the Regulation imposes specific contractual obligations on controllers when transferring personal data to third party controllers and processors which are beyond the scope of this Guidance)
4. Period for which the data will be stored (or criteria used to determine the period)
5. Existence of rights to rectification, erasure, restriction of processing, right to object to processing
6. Right to complain to the Data Protection Commission
7. Where data is not collected from the subject, information as to its source
8. Existence of automated processing or profiling, the logic involved, and the significance or consequences of such processing

There is no charge for a data access request unless the request is *'manifestly unfounded or excessive'*.

There are a number of categories of information which the insurer is entitled to redact or withhold:

- Information that is kept in contemplation of, or for the establishment, exercise or defence of, a legal claim or prospective legal claim (where it is necessary and proportionate to withhold the data in the circumstances);

- Estimates of liability in the case of a legal claim where disclosure would prejudice the commercial interests of the Controller;
- An expression of opinion about the data subject by another person given in confidence or on the understanding that it would be treated as confidential (where it is necessary and proportionate to withhold the data in the circumstances);
- Personal information that is legally privileged or which is retained by the insurer for the purpose of seeking, receiving or giving legal advice;
- Health information, subject to compliance with the Data Protection Act 2018 (Access Modification) (Health) Regulations 2022:
    - Health information that has not been provided to the insurer directly by the individual e.g. a medical report should not be made available to the individual in response to an access request if the insurer has reasonable grounds for believing that granting access to the data subject to the health data concerned would be likely to cause serious harm to the physical or mental health of the data subject.

    - Any medical information provided to the insurer by the individual directly e.g. as part of their policy application or a claim, should be provided directly to the individual as part of the access request response.

In relation to a Right of Access request being partially or wholly refused then the rationale for the refusal must be provided. The European Data Protection Board's guidelines on Data Subject Rights – Right of Access adopted on 18th January 2022 are available here.

The right to rectification

Under Article 16 of the Regulation data subjects have the right to have inaccurate personal data rectified. This right is linked to the principle of accuracy as it imposes a specific obligation to reconsider the accuracy of data when a request is received.

A request can take the form of a request to complete information a data subject believes is incomplete or a challenge to the accuracy of the data held. Insurers should have procedures in place for responding to such requests.

Insurers carry out data rectification free of charge unless the request is manifestly unfounded or excessive, in which case insurers can charge a reasonable fee for the administrative costs of complying with the request.

Insurers will respond to the request within one month. If the request is complex or if the insurer has received a high volume of requests, the time limit to respond can be extended by a further two months.

When responding to a request an insurer must request identity verification from the data subject unless identity and contact details have already been validated.

If an insurer has shared the personal data with other controllers (that the data subject has no direct contact with, such as reinsurers) and it is reasonable or feasible, the insurer should contact each recipient and inform them of the rectification or correction of the personal data (unless this proves impossible or involves disproportionate effort).

An update to personal data such as a change of address is not a correction or rectification and therefore is not within scope of this requirement. Such requests will be handled in line with the insurer's normal policy servicing procedures. (Where an insurer subsequently fails to update the personal data as requested this may subsequently need to be rectified).

The right to erasure

In accordance with Article 17 of the Regulation the data subject has the right to obtain from the controller, erasure of his or her personal data.

The right to request erasure of personal data is not an absolute right and applies in limited circumstances and is subject to restrictions. The right can apply for example:

- where the personal data is no longer necessary for the purposes for which the insurer collected them; or
- where the personal data has been processed unlawfully by the insurer.

Examples of situations where the request will not be complied with include where the processing is necessary:

- for the establishment, exercise or defence of legal claims; or
- for compliance with a legal obligation which requires the insurer to process the data. This would include situations where the insurer is legally required to retain records for a specified duration in accordance with regulatory requirements, for example, the Consumer Protection Code.

In instances where a valid right to be forgotten request is received by an insurer the insurer is obliged to erase the data without undue delay. In instances where the data has been made public by the insurer, they are also required, taking into account available technological solutions and any associated cost, to inform any other data controllers which are processing the data that the data subject has made an erasure request.

The right to data portability

Article 20 of the Regulation affords data subjects the right to data portability in certain circumstances.

The right only applies to personal data which the data subject has provided to a controller directly and which is held in an automated format.

The right to data portability provides that the data controller must provide the personal data in a structured, commonly used and machine-readable format.

The data subject has the right to transmit the data to another controller or can ask the data controller to transfer the data directly to another data controller where technically feasible.

It is important to note that the practicality of this right in an insurance context is limited. In accordance with the principles of data minimisation and accuracy it is unlikely an insurer can use a copy of personal data received from a data portability request. This is due to the fact that the insurer can only process information needed for the contract of insurance (and the information required may vary from insurer to insurer) and the requirement to have the most up to date personal data for underwriting. An insurer may therefore insist that an application form is completed. It is also important to note that insurers are not obliged to adopt or maintain processing systems which are technically compatible.

The right to object to processing of personal data

In accordance with Article 21 of the Regulation individuals have the right to object to the processing of their personal data in certain circumstances. This means data subjects can request insurers to stop processing their personal data.

To object to processing a data subject must contact the insurer and state the grounds for objection relating to their particular circumstances. If the insurer deems the objection valid they must cease processing the personal data unless compelling legitimate reasons exist as to why they need to continue processing (which may include that the processing is necessary for legal claims or for the conclusion of a contract). Therefore the right to object is not absolute and depends on the circumstances of each situation.

An objection to processing can be made verbally or in writing to the insurer. The insurer has one month to act upon the objection which can be extended by a further two months if the request is complex or the insurer has received a high volume of requests.

When responding to a request, insurers must request identity verification from the data subject. This is in order to prevent a risk of data being disclosed to the wrong person.

The right of restriction of processing

Article 18 of the GDPR affords data subjects the right to restrict the processing of their personal data in certain circumstances. This may be due to concerns about the content of the information retained by an insurer or concerns in relation to how an insurer is processing their data. A restriction may only apply for a certain period of time.

When processing is restricted, insurers may continue to store the personal data, but may use it only for certain specified purposes e.g. for the establishment, exercise or defence of legal claims.

Insurers should take reasonable steps to ensure that if the personal data has been disclosed to third parties, that the third party is informed of the restriction to the personal data. This may include informing data controllers and data processors such as brokers, outsourced service providers etc.

Once an insurer has made a decision on the accuracy of the personal data, or if the insurer's legitimate grounds override those of the individual, the restriction may be lifted provided that the data subject has been informed of the decision to remove the restriction.

Rights in relation to automated decision making, including profiling

In accordance with Article 22 of the Regulation, data subjects have a right to be informed of the existence of any automated individual decision-making (i.e. without any human involvement) including profiling. Profiling has been defined in the Regulation as any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements.

In addition to this right data subjects have a right not to be subject to a decision based solely on such methods that produces legal effects or similarly affects him/her. This right is closely linked to the right to object as per Article 21 of the Regulation which also specifically mentions profiling**.**

There are some exceptions to the above such as where this is:

- necessary for entering into or performance of a contract;
- authorised by Union/Member State law and where suitable measures to safeguard data subjects' rights, freedoms and legitimate interests are applied; or
- based on explicit consent.

Where automated decision making and/or profiling are used in the course of an insurance contract or policy insurers shall ensure the following is in place:

- suitable measures are implemented to safeguard the data subject's rights;
- data subjects are informed they have a right to have human intervention and to express point of view and contest a decision;
- that decisions will not relate to special categories of data unless certain requirements set out in Article 9 of the Regulation and section 50 of the Data Protection Act 2018 in relation to processing of special category data are met.

In accordance with the principle of transparency insurers that make automated decisions (including profiling) will tell the data subject that they are engaging in this type of activity, provide meaningful information about the logic involved and explain the significance and envisaged consequences of the processing.

Examples of the type of information that will be shared are set out below:

- the categories of data that have been or will be used in the profiling or decision-making process (including why these categories are pertinent);
- how any profile used in the automated decision-making process is built including any statistics used in the analysis;
- why this profile is relevant to the automated decision-making process and how it is used for a decision concerning the data subject;
- how the outcome of such decisions will be shared with the data subject; and
- provide information about how to request human intervention, express a view and/or to contest a decision.

Section D: Appendixes

Appendix 1: Special Provisions relating to genetic data

The Disability Act 2005 (as amended) provides that the processing of genetic data in relation to a policy of insurance (in relation to health or otherwise), life assurance, an occupational pension, a retirement annuity contract or any other pension arrangement (insurance or pension products) is prohibited.

An insurer must not request that an applicant have a genetic test as part of an insurance policy or pension arrangement.

During the process of applying for an insurance or pension product, questions about the health of an individual must not include any question about genetic tests. In addition, health questions asked directly of the individual must include a form of words bringing to his/her attention the fact that he/she should not disclose a genetic test result.

Each request to a person's GP, an independent doctor or a claims visitor to assess and/or examine an individual on an insurer's behalf, which may involve the taking of a health history other than by way of completing a standard medical examination report form, must include a form of words bringing to the doctor's attention the fact that he/she should not include any genetic test result in his/her report.

Inadvertently obtained genetic data:

Despite the inclusion of the above wordings on relevant insurance documentation, it is possible that applicants, claimants or doctors will in some instances provide genetic test results.

In the event of a genetic test result coming into the possession of an insurer, the genetic test result must be ignored and not taken account of by the insurer in any way whatsoever. This applies both to positive and negative test results.

Genetic test results coming into an insurer's possession in this way are likely to be included in the body of an application form or medical report. Ideally the genetic test results should be deleted from the paper and/or electronic file. Where this is not practical, a note should be made on the file confirming that the genetic test result has been ignored in accordance with the Disability Act 2005 (as amended).

The handling of files that include inadvertently obtained genetic test results is a sensitive matter and one which must be dealt with properly in accordance with the Disability Act 2005 (as amended). In the event that there is any doubt in relation to how such a file should be handled it should be referred to the underwriting department or the Data Protection Officer.

Appendix 2: Guidelines for disclosure of personal information to Private Investigators

Any processing of information by private investigators, when undertaken on behalf of an insurance company, in the context of the assessment of a claim or other similar reason must be undertaken in full compliance with the Regulation and the Data Protection Acts. In addition, insurers must only contract private investigators who have been licensed by the Private Security Authority (PSA) pursuant to S.I. No.195 of 2015.

The private investigator expected to comply at all times with the Regulation and the Data Protection Acts and shall not perform their functions in such a way as to cause the insurance company to breach any of its obligations under the Regulation and the Data Protection Acts.

Any unauthorised processing, use or disclosure of personal data by the private investigator is strictly prohibited.

Where the private investigator, processes the personal data of a policy holder, a claimant or other person on behalf of the insurance company, the insurance company must ensure, by way of a contract with the private investigator that the investigator shall:

- Process the personal data only in accordance with the specific documented instructions of the insurance company;
- Impose obligations of confidentiality on those who process any personal data;
- Process the personal data only as is necessary for the fulfilment of its duties and obligations under the contract with the instructing insurance company;
- Implement appropriate technical and organisational measures to protect against accidental loss, destruction, damage, alteration, disclosure or unlawful access to the personal data in their possession;
- Not sub-contract to another party without the prior written approval of the insurer (ensuring that the third party is subject to similar contractual restrictions);
- At the conclusion of each investigation or each claim (as appropriate) deliver all data collected and processed under the contract of service to the instructing insurance company and delete all such personal data held by the private investigator at that time;
- Not further disclose the personal data to any other party except with the express approval of the instructing insurance company;
- Not seek to access personal data held by other data controllers which is not in the public domain without the consent of the data subject or unless otherwise permitted by law;
- Assist the insurer in meeting any obligations to respond to data subject rights requests and in meeting its obligations in relation to data security, data breach reporting and undertaking DPIAs;
- Facilitate audits and inspections by the insurer to enable compliance validation;
- Not to use vehicle tracking devices in the conduct of their tracing or surveillance work.

Appendix 3: Personal Data that may be shared between Insurers investigating Claims

The following information (in relation to an adult or child) may be shared between insurers on request from hard-copy and/or electronic files. *Such requests may arise on foot of an initial match on InsuranceLink.* (This is relevant to non-life insurance only)

- Previous Address
- Nature/Description of Loss and/or Injury
- Amount paid to claimant
- Identity of Loss adjuster / public loss assessor
- Accident circumstances
- Location of accident
- Injury prognosis: fully recovered / on-going
- Motor assessors report on vehicle
- Category of write off
- Identity of claimant solicitor
- Claim settled: Yes / No
- Settled by: Injuries Board / solicitor / litigation / direct
- Date of settlement
- Details of whether legal proceedings were issued
- Contact phone number
- GP contact details

Appendix 4: Guidelines on Requesting "Pre-Claims" Information

The provision of "pre-claim" information, as referred to in section 1.2 of this Guidance, is as follows:

Insurers may, in respect of non-life insurance policies, only require the provision of personal data of potential claimants:

a) At a pre-claim stage in compliance with a specific legal obligation such as that contained in the Road Traffic Acts; or,

b) When the guidelines set out below are adhered to.

It is up to each insurer to ensure it is in compliance with the "pre-claim" provision of this Guidance as set out in this Appendix. However, these guidelines are intended to provide high-level guidance for insurers to consider when seeking to achieve compliance with the aforementioned "pre-claim" provision, with particular reference to employer's and public liability insurance ("liability policies"):

- It is reasonable for liability policies to require policyholders to report all incidents, irrespective of liability or the extent of the injury or damage. However liability policies should not contain conditions requiring policyholders to provide or otherwise encourage the provision of personal data of potential third party claimants or other individuals unless a third party claim has already been made or there is clear evidence that a claim is likely to be made by a potential third party claimant.
- It is reasonable to expect that a potential third-party claimant will make a formal claim where the injury is substantive or where initial information points to liability attaching to the policyholder irrespective of the severity of any injury or damage caused. Insurers should process these claims in the normal way on the basis that there is clear evidence that a claim is likely to be made by a potential third-party claimant.
- As an approximate guideline, a potential third-party claimant may not make a formal claim where an injury is minor and where initial information indicates that liability does not attach to the policyholder. Insurers should process cases falling into this category using anonymised data only on the basis that there is no clear evidence that a claim is likely to be made by the potential third party.
- Even if there is clear evidence that a claim is likely to be made by a potential third party claimant an entry must not be made on Insurance Link until a claimant takes steps indicating that a formal claim is being made.
- As mentioned above in section 1.2, where the claimant is a third party and would not otherwise have received information that could be deemed to provide for fair processing of their personal data, an appropriate fair processing notice will be made available at a suitable point in the business process, for example when issuing the first communication to claimant or their solicitor. The notice reflects the advice contained in the Article 29 Working Party (now the European Data Protection Board (EDPB) Guidance on Transparency.