Implementing the New General Data Protection Regulation

The introduction of the General Data Protection Regulation ('GDPR') changes data protection law in Europe. We understand you may have questions about Cigna's role from a data protection perspective, and about the obligations that the GDPR imposes on Cigna.

Cigna has analysed the impact of the GDPR on its operations and is putting all necessary compliance measures in place. As a result, and given our role as a controller of personal data under the law, no additional contractual provisions are required to be in place between Cigna and its clients. This includes due diligence requirements and audit provisions, which are not prescribed by the law for these circumstances. Regardless, we remain committed to collaborating in an effective way with our customers and partners to ensure the privacy and protection of their sensitive data.

Regulation scope

Concepts of the 'controller' and the 'processor' underpin existing European data protection law. These terms are used to describe the roles of the entities involved in the processing of personal data and remain central to the GDPR.

A 'controller' is the entity which determines the purposes and means of the processing of personal data – in other words, it decides how and why personal data is processed. In contrast, a 'processor' processes personal data only on behalf of the controller and in accordance with the controller's instructions. Although the GDPR does impose some obligations directly on processors, the bulk of its requirements fall to controllers.

Unless we have informed you otherwise in the agreement we have with you, we process the personal data needed to provide our services to you as a controller.

We understand that you have chosen to work with us, in part, because of the protection we provide to you and your employees' highly sensitive personal data. With this in mind, please be assured that where we are subject to the GDPR, we are fully committed to compliance with the obligations to which we are subject as controllers.

Therefore, in-line with our obligations under the GDPR, we will:

- **Process personal data fairly, transparently and on lawful grounds.** We will ensure that individuals are informed about the collection and use of their personal data, that we have a lawful basis for processing personal data, and that we process special categories of personal data (such as information about individuals' health) is aligned with the requirements of applicable data protection law. For example, where we are required to collect explicit consent for the processing of an individual's health data, we will do so. Please note, however, that the laws of some Member States permit the processing of certain types of special category personal data for insurance purposes without explicit consent.

- **Process personal data only for the purposes for which it was collected and not process it in a manner which is incompatible with those purposes.** If we process personal data for a new purpose, we will ensure that that processing is

compliant with the GDPR. In practice, this may mean obtaining individuals' consent for the new processing activity.

- **Take steps to ensure that personal data is adequate, relevant and limited to what is necessary for the purposes for which it is processed** and **accurate and updated when necessary.**

- **Implement appropriate technical and organisational measures to protect the personal data we process.** The security measures we put in place account for a number of factors including, for example, the state of the art, the nature, scope, context and purposes of our processing, and the risk our processing poses to individuals, etc. The technical safeguards we apply are also aligned with industry security standards. In addition, we will ensure that our sub-contractors implement appropriate security measures, and that they are bound by contracts which are consistent with the requirements of the GDPR.

- **Practice data protection by design and default** and **conduct privacy impact assessments where required.**

- **Ensure that personal data is adequately protected when it is transferred to destinations outside the European Economic Area.** For example, Cigna has in place an intra-group data transfer agreement incorporating the European Commission's approved standard contractual clauses to legitimise the transfer of personal data between members of the Cigna corporate group.

- **Retain personal data only for as long as is necessary for the purposes for which we process it.**

- **Honour individuals' rights in relation to their personal data.** For example, if we process an individual's personal data in the context of the provision of our services, we will respond to any requests we receive from that individual relating to their personal data.

- **Ensure that we can demonstrate 'accountability'.** We maintain policies and procedures to assist us in meeting applicable legal and regulatory standards. Key policies are maintained at global level and where appropriate, Cigna business units create and maintain department-specific compliance policies and procedures which are revised and updated on a periodic basis.

If you have any questions about our personal data handling practices, please contact GDPR@Cigna.com.

5.00.000 (0115)