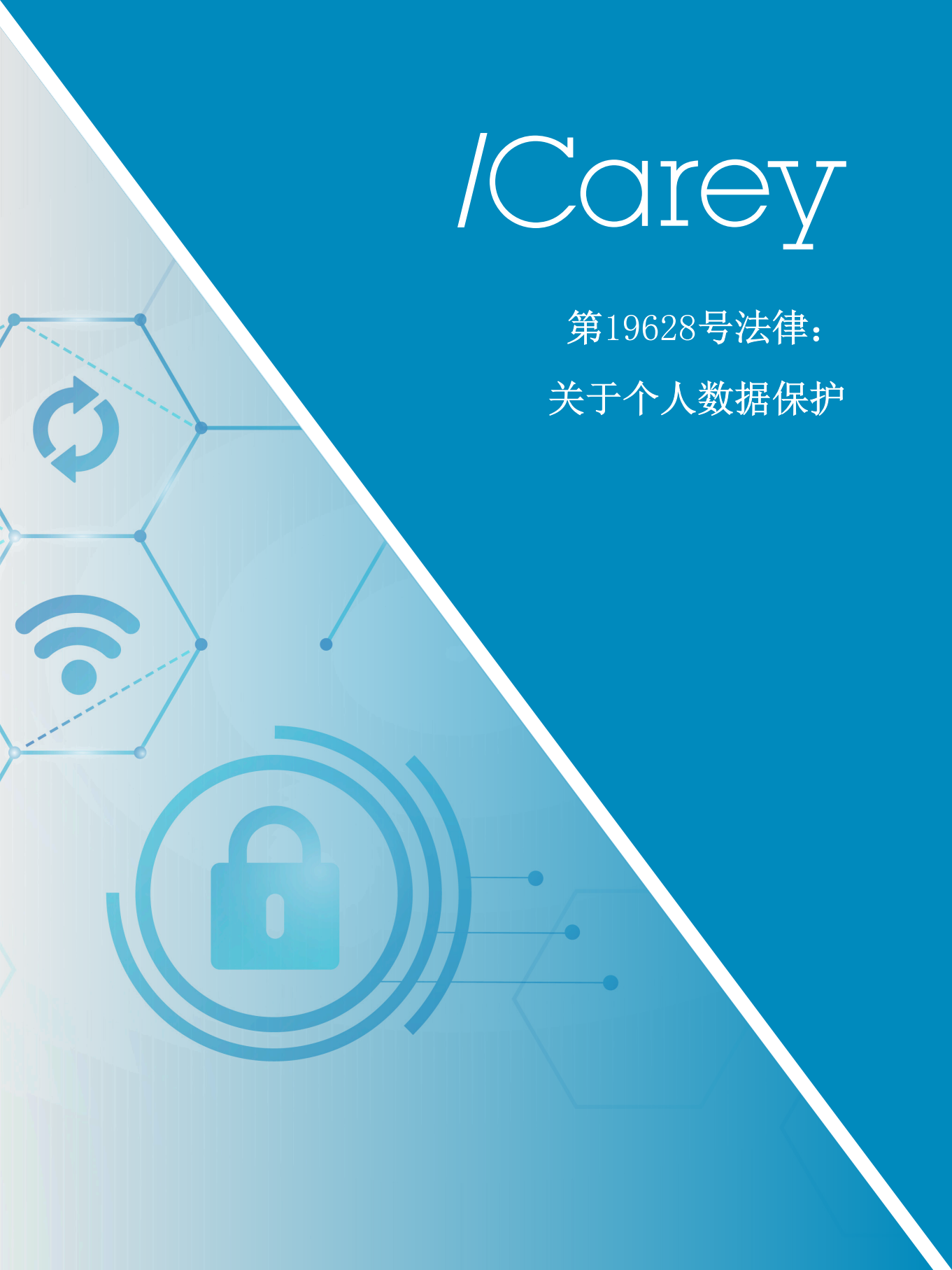
/Carey

第19628号法律：关于个人数据保护



正在讨论的法案：

序章

总则

第一条 适用对象及范围。为了规范个人数据处理活动，保护自然人个人数据权益，根据《智利共和国政治宪法》第十九条第四款规定，特制定本法。

由自然人或法人（包括公共机构）进行的所有个人数据处理活动都必须尊重个人的权利和自由，并遵守本法的规定。

依法行使言论自由和新闻自由过程中进行的数据处理活动，必须遵守《智利共和国政治宪法》第十九条第十二款的规定，不适用于本法。社交媒体除言论和新闻之外的目的而进行的数据处理活动必须遵守本法规定。

本法的规定不适用于自然人就其个人活动进行的数据处理。

第一条之二 适用的地域范围。有下列情形之一的个人数据处理活动，可适用本法：

（一）在智利境内设立或成立的数据控制者或第三方代理人。

（二）在智利境内设立或成立的数据控制者委托在任何地点设立或成立的第三方代理人进行个人数据处理活动。

（三）未在智利境内设立的数据控制者或第三方，但其个人数据处理活动旨在向智利境内的数据主体提供付费或免费的商品或服务；或监控智利境内数据主体的行为，包括行为分析、跟踪、剖析或预测。

本法律也适用于不在智利境内设立但根据合同或国际法因进行个人数据处理活动而适用于本国法律的数据控制者。

定义

第二条 依据本法，下列用语的含义为：

（一）数据存储：在登记册或数据库保存或保管数据。

（二）数据冻结：暂时中止已存储数据的任何处理操作。

（三）个人数据传输：数据控制者以任何方式将个人数据告知除数据主体以外的其他人，而无需实际转让或转移这些数据。

（四）过期数据：满足条件或有效期届满，或无明文规定但既定事实或情况发生变化，根据法律规定已失去效力的数据。

（五）统计数据：数据本身或数据处理后与已识别或可识别数据主体无关联的数据。

（六）个人数据：与已识别或可识别的自然人有关的任何信息。可识别的自然人指可以直接或间接识别的任何人，特别是可通过其姓名、身份证号码、特定身体特征、生理、遗传、心理、经济、文化或社会身份等相关的一个或多个因素识别人员的。

（七）敏感个人数据：指涉及个人身体特征、道德特征、私生活或隐私的事实或情况的个人数据，例如：民族或种族、政治、工会或行业协会、社会经济状况、意识形态或哲学信仰、宗教信仰、与健康有关的数据、人体生物学特征、生物识别数据，以及与自然人的性生活、性取向和性别认同相关的信息。

（八）清除或删除数据：以任何方式销毁存储在登记册或数据库中的数据。

（九）公开来源：任何人都可以合法访问或查询的所有数据库或个人数据集，例如《国家公报》、媒体或法定公共登记册。处理公开来源的个人数据应遵守本法规定。

（十）公共机构：《智利共和国政治宪法》所描述和规范的当局、国家机关和单位，以及第18575号法律《国家行政机关组织总法》第一条第二款中所列的机构。

（十一）匿名化：不可逆的数据处理过程，由于链接、关联或识别个人信息的链接已被销毁或消除，经过匿名化处理的数据无法与任何个人关联到一起，也不能识别其身份。匿名化数据不再是个人数据。

（十二）假名化：假名化是指对个人数据的处理，在不使用额外信息的情况下，个人数据不能再归属于特定的数据主体，条件是这种额外信息是单独保存

的，并受制于技术和组织措施，以确保个人数据不归属于一个已识别或可识别的自然人。

（十三）个人数据库：有组织的个人数据集，无论其创建、存储、组织和访问的目的、方式或形式如何，都允许数据相互关联并进行处理。

（十四）数据控制者：在个人数据处理活动中，自主决定处理目的、处理方式的任何自然人或法人，公法人或私法人，无论数据是由其直接处理还是通过第三方处理。

（十五）数据主体：个人数据所涉及的已识别或可识别的自然人。

（十六）数据处理：以任何方式收集、处理、存储、传播、传输或使用个人数据或个人数据集的任何操作或联合操作或技术手段（无论是否自动化）。

（十七）同意：数据主体、其法定代表或代理人（视情况而定）通过声明或明确的肯定性行动表达的任何自愿的、具体的、明确的和知情意愿授权处理与其有关的个人数据。

（十八）知情权：数据主体有权要求数据控制者告知其个人数据处理情况，并访问这些数据（如果适用）以及本法规定的信息。

（十九）更正权：数据主体发现其个人数据不准确、过时或不完整时，有权通过数据控制者获得修改和完善其个人数据的权利。

（二十）删除权：数据主体有权依法向数据控制者请求并获得删除或消除其个人数据的权利。

（二十一）异议权：数据主体有权依法向数据控制者请求并获得对特定数据不进行处理的权利。

（二十二）个人数据携带权：数据主体有权向数据控制者获取其个人数据的结构化、通用和常用电子格式的副本，其副本可在不同系统中运行并能够转移到其他的数据控制者。

在技术手段可行的情况下，数据主体有权将其个人数据在数据控制者之间直接转移。

（二十三）个人数据转让：个人数据从一个数据控制者转移到另一个数据控制者。

（二十四）生成主体账户：任何形式的个人数据自动化处理，包括使用个人数据对自然人的职业、经济状况、健康、个人喜好、兴趣、忠诚度、行为、位置或行踪等方面进行评估、分析或预测。

（二十五）第三方代理人或负责人：代表数据控制者处理个人数据的自然人或法人。

（二十六）监管机构：个人数据保护监管局。

（二十七）国家处罚与合规登记册：由个人数据保护监管局来管理的一个公共性质的国家登记册，记录通过认证的预防模型、采用该模型的数据控制者以及对违法数据控制者的处罚。

第三条 原则。个人数据的处理必须遵循下列原则：

（一）合法和公正原则。个人数据只能合法且公正地处理。

数据控制者必须能够证明其进行的个人数据处理活动的合法性。

（二）目的原则。必须出于特定、明确和合法的目的收集个人数据。个人数据的处理仅限于这些目的。

在应用这一原则时，不得出于收集时告知的目的以外的其他目的处理个人数据，除非有以下情形之一的：处理目的与初始目的相符；数据主体和数据控制者之间存在合同或先合同关系，只要处理目的符合合同约定或与先合同的讨论或谈判一致，证明出于不同目的处理数据是合理的；数据主体在法律规定的情况下再次同意的。

（三）相称性原则。处理的个人数据必须严格限于与处理目的有关的必要、充分和相关的数据。

个人数据只能在实现处理目的所需时间内保留，逾期后必须将其删除或匿名化，法律规定的例外情况除外。若需保留更长时间，需要征得数据主体的合法授权或同意。

（四）质量原则。个人数据必须准确、完整、最新且与其来源和处理目的相关。

（五）责任原则。处理个人数据的相关责任人须遵守本条所列原则并依法承担义务和责任。

（六）安全原则。在处理个人数据时，数据控制者必须保证足够的安全标准，保护数据免遭未经授权或非法处理，防止意外丢失、泄露、破坏或毁坏。安全措施必须适当并与处理方式和数据本身的性质相符。

（七）信息透明原则。数据控制者必须向数据主体提供行使本法规定的权利所必需的所有信息，包括处理个人数据的政策和做法，这些信息必须以精确、清晰、明确和免费的方式能够永久访问，或提供给任何相关方。

数据控制者必须采取适当和及时的措施，使数据主体能够访问本法规定的所有信息，以及与所进行的数据处理相关的任何其他通信。

（八）保密原则。个人数据控制者和有权访问数据的人必须对数据保密。数据控制者须建立充分适当的控制措施予以保密。即使与数据主体关系终止后，该义务仍然存在。

第一章

个人数据主体的权利

第四条 数据主体的权利。任何人自行或通过其法定代表人或代理人（视情况而定）均享有本法规定的个人数据知情权、更正权、删除权、异议权、携带权和冻结权。

这些权利属于个人权利，不可转让、不可剥夺，并且不受任何法案或公约限制。

自然人死亡的，可由其继承人行使本法规定的相关数据主体权利。

死者生前明确禁止或法律规定的，继承人将无法访问死者的数据，也无法要求更正或删除数据。

第五条 知情权。数据主体有权要求数据控制者告知其个人数据处理活动情况，并访问所述数据和下列信息：

（一）所处理的数据及其来源。

（二）数据处理目的。

（三）数据接收方的类别、级别或类型，已经或将向其传输或转让个人数据的接收方的身份（如果数据主体要求）。

（四）个人数据将被处理的时间期限。

（五）依照本法第十三条第四项规定处理数据时，数据控制者的合法权益。

（六）数据控制者依照本法第八条之二进行数据处理所应用逻辑的重要信息。

数据控制者始终有义务提供信息并允许访问所请求的数据，法律另有明确规定的除外。

第六条 更正权。数据主体发现其个人数据不准确、过时或不完整时，有权在数据控制者处更正与其相关或正在处理的个人数据。

更正后的数据必须传达给数据控制者之前已传达或转让相关数据的个人、实体或组织。

一旦更正完成，未经更正请求，数据将不得再次进行处理。

第七条 删除权。数据主体有权要求数据控制者删除与其相关的个人数据，尤其在下列情形下：

（一）数据对于收集或处理时的目的已经不再必要。

（二）数据主体已撤回对其个人数据进行处理的同意，且无其他法律依据支持数据处理。

（三）数据被控制者非法获取或处理。

（四）已过期的数据。

（五）因履行司法裁决、数据保护机构决议或法律义务而必须删除的数据。

（六）再无其他法律依据支持数据的处理，数据主体可根据下列条款行使异议权。

下列必要情形，不宜行使数据删除权：

1. 为了行使言论和信息自由权；

2. 为了履行法律义务或数据控制者与数据主体之间签订的合同；

3. 为了履行公共职能或开展符合公共利益的活动；

4. 出于公共卫生领域的公共利益需求，依照法律规定的条件和保障条款而需执行的；

5. 出于历史、统计或科研，以及为公共利益研究或调查的目的；

6. 出于提起、执行行政或司法诉讼或抗辩的目的。

第八条 异议权。有下列情形之一的，数据主体有权反对数据控制者对其有关的个人数据进行具体或特定处理：

（一）数据处理合法性的基础是满足数据控制者的合法权益，数据主体可以随时行使其异议权，且数据控制者必须停止处理其个人数据。除非数据控制者有充分的法律依据证明其优先于数据主体的利益、权利和自由的，或者提起、执行诉讼或抗辩的。

（二）根据本法第八条之二，数据处理完全是为了商品、产品或服务的直接营销的，包括生成主体账户。

（三）处理公开来源数据且无其他法律依据支持数据处理的。

出于科研、历史、统计目的，履行公共职能或开展公共利益活动所必需的个人数据处理，不得行使异议权。

第八条之二 自动化个人决策，包括生成主体账户。数据主体有权反对且不受基于对其个人数据自动化处理决策（包括生成主体账户）结果的约束，且这些决策结果对数据主体可能造成法律后果或产生重大影响。

下列情形不适用前款规定：

（一）数据主体与数据控制者签订或执行合同需要自动化决策的；

（二）依照本法第十二条规定事先取得数据主体的明确同意的；

（三）法律规定的，只要规定使用保障措施来保护数据主体的权利和自由。

所有基于个人数据自动化处理决策的情形，包括前款第一、二、三项的情

形，数据控制者必须采取必要措施以确保数据主体的权利、自由、知情权和透明度权、获得解释权、人为干预权、观点表达权，以及要求对自动化决策进行检查的权利。

第八条之三 冻结权。无法确定其准确性或有效性存疑且不适用删除的，数据主体有权要求暂停任何个人数据处理操作。

第九条 个人数据携带权。数据主体有权索取和接收一份已提供给数据控制者与其有关的个人数据副本，该副本采用电子的、结构化的、通用的和常用的格式，可在不同系统中运行。满足下列情形时，副本可传输或转移到其他数据控制者：

（一）副本转移处理以自动化方式进行，且

（二）副本转移处理拥有数据主体的同意。

数据控制者必须使用最快捷、最轻松的方式，不得妨碍或阻碍该项权利的行使。

数据控制者还必须以清晰准确的方式向数据主体告知获取其个人数据的必要措施，并说明执行这些操作的技术特征。

在技术手段可行的情况下，数据主体有权将其个人数据在数据控制者之间直接转移。

行使携带权并不意味着转移前的数据被删除，除非数据主体在请求携带权时明确提出需同时删除数据的要求。

第十条 数据主体行使权利的形式和方式。本法规定的权利由数据主体对数据控制者行使，数据主体的个人数据由不同的数据控制者处理的，数据主体可以向其中任何控制者行使其权利。

未在智利设立的数据控制者必须在监管机构备案并以书面形式指定一名本国居民为其代表，以便数据主体可以行使本法规定的权利以及处理可能发生的来文和司法或行政通知。

数据控制者必须采取技术手段和工具，使数据主体能够迅速、灵活和高效地行使其权利。数据控制者提供的方法必须操作简单。

更正权、删除权和异议权的行使对数据主体永远是免费的。知情权可至少每

季度免费行使一次。

当数据主体在一个季度内不止一次行使其知情权和携带权时，数据控制者只能要求其支付所产生的直接费用。在本法第二十七条第六项情形下，数据控制者不得要求其支付该笔费用。

因行使前款所述权利而产生的成本的参数和机制由监管机构发布一般性指示来确定，其中需要考虑要交付的数据量、法律性质以及数据控制者所在实体或公司的规模。

监管机构必须确保数据主体根据本法规定有效行使和落实本法赋予数据主体的权利。

第十一条 数据控制者受理程序。为行使本法规定的权利，数据主体必须向数据控制者提交书面请求，发送至专门的电子邮件地址或等效电子媒介。申请必须至少包含下列内容：

（一）数据主体及其法定代表人或代理人（视情况而定）的身份证明及根据监管机构制定的程序、方式和方法进行的身份认证。

（二）指明邮寄地址或电子邮件地址或其他等效媒介，用于沟通答复。

（三）明确行使相应权利对应的个人数据和确定的处理方式。

（四）有更正请求的，数据主体必须指明要进行的准确修改或更新，必要时附上佐证。有删除请求的，数据主体必须指明援引的理由并附上佐证（如果适用）。有异议请求的，数据主体必须指明援引理由，有本法第八条第一项之情形的，数据主体必须简要证实其请求，还可附上自认为适当的佐证。有知情请求的，数据主体提供身份证明即可。

收到请求后，数据控制者必须确认收到请求，并在自收到请求之日起十五个工作日内作出答复。

数据控制者必须以书面形式回复至数据主体的邮寄地址或电子邮件地址。数据控制者必须做好存储备份，以证明到对相应邮寄地址或电子邮件地址的回复、日期及其全部内容。

拒绝接受全部或部分请求的，数据控制者必须根据其决定，指明依据和佐证。此情况下，数据控制者必须通知数据主体，在十五个工作日内数据主体可以

依照本法第四十一条的规定向监管机构提出诉讼。

在前款第二款规定的十五个工作日后，数据控制者未作答复的，数据主体可依前款规定，直接向监管机构提出诉讼。

提出更正、删除或异议请求的，数据主体有权向数据控制者要求并获得对其数据或处理活动（视情况而定）的临时冻结权。临时冻结的请求必须有正当理由，数据控制者必须在收到请求后两个工作日内给予回应。只要临时请求未得到解决，数据控制者将无法处理数据主体的数据。数据的临时冻结不会影响数据控制者的存储。如果拒绝接受请求，数据控制者必须说明理由，并以电子方式将其决定报告给监管机构。数据主体可根据本法第四十一条第一项的规定，对此决定向监管机构提出诉讼。

数据处理的更正、删除或反对仅适用于收到请求的数据控制者。数据控制者已将上述数据传输给他人的，必须将因更正、删除或异议而发生的变更再次告知他人。

数据主体可以提供任何有助于个人数据检索的其他背景信息。

第二章

个人数据及特殊类别数据的处理

第一节

数据主体的同意、数据控制者的义务和职责及一般数据处理

第十二条 数据处理的一般规定。经数据主体同意，处理与数据主体相关的个人数据是合法的。

数据主体的同意必须真实自愿、充分知情及明确具体。同意也必须事先通过口头、书面或等效电子媒介表示，或通过明确数据主体意愿的肯定行动予以明确。

代理人作出同意的，代理人需明确有权为之。

数据主体可以随时使用与做出同意时使用的类似或等效方式来撤销同意，无需任何理由。撤销同意不具有追溯效力。

用于做出或撤销同意的方式必须便捷、可靠、免费，且数据主体可以随时使用。

数据控制者在执行合同框架内收集数据或提供不需要进行此类收集服务的，默认无需取得处理数据的自愿同意。

以同意处理数据为唯一交换，提供商品、服务或者利益的，不适用上款规定。

数据控制者有义务证明其已获得数据主体的同意，并且数据处理应以合法、公开和透明的方式进行。

第十三条 合法处理数据的其他情形。有下列情形之一的，未经数据主体同意，对个人数据的处理是合法的：

（一）根据本法第三章的规定，处理涉及与经济、金融、银行或商业性质义务有关的数据。

（二）执行或履行法律义务或根据法律规定而处理的数据。

（三）签订或执行数据主体与数据控制者之间的合同，或执行应数据主体要求采取的合同前措施所必要的数据处理。

（四）不影响数据主体的权利和自由，满足数据控制者或第三方合法利益必要的数据处理。任何情形下，数据主体都可以随时要求了解涉及到本人数据处理以及进行对应处理所依据的合法权益。

（五）在法院或公共机构表达、行使或捍卫权利时必要的数据处理。

数据控制者必须证明数据处理的合法性。

第十四条 数据控制者的义务。在不影响本法其他规定的情况下，数据控制者具有下列义务：

（一）告知数据主体并提供信息证明其进行数据处理的合法性，且在需要时能够迅速提供上述信息；

（二）确保出于特定、明确和合法目的从合法访问来源收集个人数据，并且其处理仅限于这些目的；

（三）根据本法规定，传输或转让准确、完整和最新的信息；

（四）删除或匿名化为执行先合同措施而获得的数据主体的个人数据；

（五）遵守履行本法规定的关于个人数据处理的其他职责、原则和义务。

不在智利拥有注册地址并处理智利本国境内数据主体数据的数据控制者必须指明一个电子邮件地址或其他合适的联系方式，并对其保持更新，以便接收来自数据主体和监管机构的来文。

第十四条之二 保密义务。数据控制者有义务对与数据主体有关的个人数据保密，除非数据主体已明确公开这些数据。即使与数据主体结束关系后，该义务仍然存在。如果数据控制者对从公开来源获得的个人数据执行任何操作，例如：根据某些标准对其进行组织或分类，或者将其与其他数据合并或补充，该操作所生成的个人数据受保密义务的保护。

保密义务不妨碍数据控制者应数据主体和公共机构在其法定权限范围内必须依法进行的数据传输或转让，以及履行向数据主体提供访问权限和告知数据来源的义务。

数据控制者必须采取必要措施，以确保执行数据处理的雇员或自然人或法人在其职责范围内遵守本条规定的保密义务。

本法第二十四条所提及的个人、机构及其雇员要求和发送上述信息的，亦有保密义务。

第十四条之三 信息透明义务。数据控制者必须在其网站上或以任何其他等效信息方式向公众永久提供至少下列信息：

（一）已采用的个人数据处理政策及其日期和版本；

（二）数据控制者及其法定代表人的身份，以及数据保护专员的身份（若有）；

（三）可以收到数据主体提出请求通知的邮寄地址、电子邮件地址、联系方式或常用且易于访问的等效技术媒介和标识；

（四）所处理数据的类别、级别或类型；数据库涉及群体的一般描述；预期向其传输或转让数据的接收者，和处理的目的；处理的合法依据；数据处理所基于的合法权益；

（五）为保护其管理的个人数据库而采取的政策和安全措施；

（六）协助数据主体依法向数据控制者请求访问、更正、删除、异议和携带个人数据的权利；

（七）数据控制者拒绝或未及时回应所提出请求的，协助数据主体向监管机构提出诉讼的权利；

（八）必要时，个人数据转移到第三国或国际组织时，应提供足够的保护。如果未能达到足够的保护标准，则必须报告并证明这种转移的合理性；

（九）个人数据的保存期限；

（十）个人数据的来源，以及在相应情况下是否来自公开渠道；

（十一）基于数据主体同意处理数据的，数据主体有权随时撤回同意，但不影响撤回前基于数据主体同意已进行的数据处理的合法性；

（十二）有自动化决策的，包括主体账户的生成。应通报有关应用逻辑的重要信息以及该处理对数据主体的预期后果。

第十四条之四 设计和默认保护义务。为了遵守本法规定的数据主体的原则和权利，数据控制者在处理个人数据之前和期间必须在设计上采取适当的技术和组织措施。

所采取的措施必须考虑到技术水平、实施成本、数据处理的性质、范围、背景和目的，以及与上述活动相关的风险。

数据控制者需考虑收集的数据数量、处理范围、保存期及可达性，采取必要的技术和组织措施，以确保在默认情况下仅处理上述活动特定且绝对必要的个人数据。

第十四条之五 采取安全措施的义务。综合考虑当前的技术水平和应用成本，以及处理的性质、范围、背景和目的，以及与处理的数据类型相关的风险概率及其影响的严重程度，数据控制者必须采取必要的安全措施来保障遵守本法规定的安全原则。数据控制者采取的措施必须确保数据处理系统的机密性、完整

性、可用性和弹性，且必须避免其被更改、破坏、丢失、擅自处理或擅自访问。

考虑到技术水平、应用成本、处理的性质、范围、背景和目的，以及对数据主体的权利和自由的风险概率和影响的严重程度，数据控制者和数据处理者必须采取适当的技术和组织措施来确保与风险相适应的安全级别，视情况要包括：

（一）个人数据的假名化和加密；

（二）确保数据处理系统和服务持续保持机密性、完整性、可用性和弹性的能力；

（三）发生物理或技术事故时，有快速恢复可用性和访问个人数据的能力；

（四）为了确保处理的安全性，定期验证、评估和评价技术和组织措施有效性的过程。

一旦发生安全事故，如果存在司法或行政诉讼，数据控制者当事人有义务证明其基于风险程度和可用技术所采取的安全措施及运行情况。

第十四条之六 报告违反安全措施行为的义务。数据控制者必须尽可能迅速且不得无故拖延向监管机构报告违反安全措施所造成的个人数据或通信的破坏、泄漏、丢失或意外或非法更改，或非法访问数据使数据主体的权利和自由存在可能风险的行为。

数据控制者必须记录这些通知，说明所发生的违规行为的性质、影响、数据类别和受影响的数据主体的大概数量，以及为管理和防止未来事故而采取的措施。

上述违规行为若涉及敏感个人数据、与十四周岁以下儿童有关的数据或与经济、金融、银行或商业性质的有关的数据，数据控制者还必须通知到这些数据主体，适当时可通过他们的代表予以通知。通知必须清晰简单，确定受影响的数据、安全漏洞的可能后果以及所采用的解决方案或保护措施。通知必须发给每个受影响的数据主体，如果无法实现，将通过大众媒体在全国范围内传播或发布通知的方式来完成。

本条所述信息义务不妨碍其他法律规定的其他信息义务。

第十四条之七 差异化合规标准。为遵守本法第十四条之三和之五规定的信息和安全义务而对数据控制者要求的最低标准或条件，分别根据相关数据的类

型、数据控制者所在实体或公司的规模（如果数据控制者是自然人或法人，实体或公司的规模根据第20416号法律《为小公司制定特殊规则》第二条规定的类别确定）、开展的活动以及处理的个人数据的数量、性质和目的来确定。

前款所指的合规标准或最低条件及差异化措施，由监管机构通过一般性指示确定。

第十五条 个人数据转让。经数据主体同意的，个人数据可以转让以实现处理目的。履行和执行数据主体作为当事方的合同所必需转让的或者符合本法第十三条第四项规定的条件转让方或受让方有合法权益的并按法律规定的，个人数据也可以转让。

已取得的数据主体的同意但未涉及数据转让的，在数据转让操作之前从法律角度必须重新取得数据主体的同意。

数据转让必须以书面形式或通过任何合适的电子方式记录在案。记录应包括当事方的身份信息，转让的数据，处理的预期目的以及转让方和受让方约定的其他内容或规定。

受让方必须依照转让合同中规定的目的对转让的个人数据进行处理。

一旦转让完成，受让人获得法律角度的数据控制者的身份。对于其继续执行的处理操作，转让方同样保持数据控制者的身份。

一旦经过必要验证，证实数据转让未取得数据主体的同意，则转让无效，并且受让人必须删除所有收到的数据，不影响相应法律责任的承担。

第十五条之二 通过第三方进行数据处理。数据控制者可以直接或通过第三方进行数据处理。通过第三方处理的，第三方根据数据控制者的命令和指示处理个人数据，禁止将其用于与数据控制者约定的目的以外的用途，未经数据控制者明确具体授权不得进行数据转让或移交。

第三方将数据用于约定的目以外的用途，或未经前款规定的授权而转让或移交数据的，从法律角度第三方将被视为数据控制者，必须亲自为其造成的违规行为负责，并与数据控制者一起对就所造成的损害依法承担连带责任，不影响与第三方或数据控制者相对应的合同责任。

通过第三方处理数据受数据控制者与第三方遵照现行法律签订的合同的约束。合同必须规定委托任务的目的、期限、数据处理目的、处理的个人数据类

型、数据涉及的数据主体类别以及双方的权利和义务。除非有数据控制者的具体书面授权，第三方不得将部分或全部委托任务再次委托给其他方。若已再次委托，第三方对委托任务继续承担连带责任，不能以委托处理为由免除责任。监管机构将在其网站上向公众提供合同范本。

第三方必须遵守本法第十四条之二、之四、之五的规定。本法第十四条之七第一款所规定的差异化安全标准，亦适用于第三方。违反安全措施的，第三方必须将此报告给数据控制者。

一旦第三方完成处理服务，其所拥有的数据必须视情况予以删除或返还给数据控制者。

第十五条之三 个人数据保护影响评估。由于其性质、范围、背景、采用的技术或目的，某种数据处理可能对数据主体的权利产生高风险的，数据控制者在处理操作开始之前必须先评估该处理对个人数据保护的影响。

下列情形之一的，始终需要进行影响评估：

（一）基于数据处理或自动化决策（例如：生成主体账户）对数据主体的个人方面进行系统和详尽的评估，并对其产生重大法律影响。

（二）大规模数据处理。

（三）涉及对公共区域进行系统观察或监控的数据处理。

（四）在同意的例外情况下处理敏感和受特别保护的数据。

数据保护监管局将建立并发布一份指导条例，列出需要与否对个人数据保护进行影响评估的处理操作类型。该监管机构还将制定执行此评估的最低准则，该准则至少要考虑对处理操作的说明、处理目的、必要性和相称性的评估、风险评估和缓解措施。

若根据评估结果证明某数据处理具有高风险，数据控制者可以向数据保护监管局咨询以获得建议。

第二节

敏感个人数据处理

第十六条 敏感个人数据处理的一般规定。敏感个人数据的处理只能在所涉及数据主体通过书面或口头声明或同等技术手段明确表示同意的情况下进行。

有下列情形之一的，未经数据主体同意，处理敏感个人数据是合法的：

（一）处理涉及数据主体已明确公开的敏感个人数据，并且其处理与这些数据的公开目的相关。

（二）非盈利公法人或私法人基于其合法权益进行数据处理，并满足下列条件：

1. 用于政治、哲学、宗教、文化、工会或行业协会目的；

2. 数据处理只涉及其成员或关联方；

3. 数据处理的目的是为了实现其机构的特定目的；

4. 法人提供必要的保障以防止泄露、盗窃或未经授权使用或处理数据；

5. 个人数据不会传输或转让给第三方。

符合上述条件，法人不需要数据主体的同意即可处理其数据，包括敏感个人数据。如有疑问或发生行政或司法诉讼，数据控制者必须证明上述条件成立。

不再是法人主体的成员的数据必须匿名或删除。

（三）数据处理对于保护数据主体或其他人的生命、健康或身心完整至关重要，或者数据主体因身体或法律原因无法同意。一旦障碍消除，数据控制者必须详细告知数据主体所处理的数据和所执行的具体处理操作。

（四）在法院或公共机构表达、行使或捍卫权利必要的数据处理。

（五）数据控制者或数据主体在劳动或社会保障领域行使权利和履行义务所必需的依法实施的数据处理。

（六）法律明确授权或强制执行的敏感个人数据处理。

本条所提及的未经同意处理数据的例外情况，是指适用于不具有敏感性质的数据处理。

第十六条之二 与健康和人体生物学特征相关的敏感个人数据。符合本法第十六条第一款的规定，专门用于卫生法规定的目的，与数据主体健康相关的个人数据，以及与数据主体生物学特征相关的数据，例如：遗传数据、蛋白质组数据或代谢数据。

未经数据主体同意，只有在下列情形之一的，才能依照本法规定的原则和规定处理与数据主体健康及其生物学特征相关的敏感个人数据：

（一）数据处理对于保护数据主体或其他人的生命、健康或身心完整至关重要，或者数据主体因身体本身或法律原因无法同意的。一旦障碍消除，数据控制者必须详细告知数据主体所处理的数据和所执行的具体处理操作。

（二）法定健康预警时。

（三）出于历史、统计或科研目的，服务于公共利益或造福人类健康的调查研究，或用于开发其他方式无法开发的医疗产品或用品的。使用与健康或生物学特征相关的个人数据的科学研究结果可以自由发表或传播，发布的数据必须事先匿名。

（四）在法院或行政机构表达、行使或捍卫权利必要的数据处理。

（五）为了预防医学或职业医学、工人工作能力评估、医学诊断、提供健康或社会护理或治疗、或健康和社会护理系统和服务管理而必需的数据处理。

（六）法律允许并明确处理目的的。

当数据或样本收集来源于工作、教育、体育、社会、保险、安全或身份识别领域时，禁止处理和转让与数据主体的健康和生物学特征相关的数据以及与已识别或可识别人员相关的生物样本，包括存储生物材料。法律明确规定在符合条件的情况下进行处理且涉及本条所提及的任一情形除外。

本条所提及的未经同意处理数据的例外情况，是指适用于不具有本条所指特殊性质的数据处理。

第十六条之三 生物识别性质的敏感个人数据。具有生物识别性质的敏感个人数据是指通过特定技术处理获得的与个人的身体、生理或行为特征相关的能够用于身份识别的数据，例如：指纹、虹膜、手部或面部特征及声音。

数据控制者依照本法第十六条第一款的规定，且向数据主体提供下列特定信息，才能处理这些数据：

（一）所采用的生物识别系统；

（二）生物识别系统收集的数据的具体用途；

（三）生物特征数据的使用期限；

（四）数据主体行使权利的方式。

只有在本法第十六条之二第二款所述的情况下，才可未经同意处理个人生物识别数据。

第三节

特殊类别个人数据处理

第十六条之四 与儿童和青少年有关的个人数据。处理有关儿童和青少年的个人数据，要立足儿童和青少年的最大利益，尊重儿童和青少年的渐进自主性。

依照前款规定，处理儿童的个人数据，必须取得其父母或法定监护人或儿童个人护理负责人的同意。法律明确规定或法律强制的除外。

青少年的个人数据可依照本法规定的成人授权规则进行处理，下款规定的除外。

十六周岁以下青少年的敏感个人数据处理，必须取得其父母或法定监护人或未成年人个人护理负责人的同意。法律明确规定或法律强制的除外。

就本法而言，儿童指十四周岁以下，青少年是指年满十四周岁未满十八周岁。

教育机构和所有处理或管理儿童和青少年个人数据的个人、公共或私人实体

具有确保合法使用和保护有关儿童和青少年的个人信息的特殊义务。

第十六条之五 用于历史、统计、科研为目的的个人数据。当数据处理仅用于服务于公共利益的历史、统计、科研目的以及调查研究时，自然人、公法人或私法人（包括公共机构）对个人数据的处理具有合法权益。

数据控制者必须采取并证明其已遵守所有必要的质量安全保证措施，以确保数据仅用于此类目的。数据控制者必须识别敏感个人数据处理造成的可能风险并采取旨在减少或缓解风险的措施。一旦满足这些条件，数据控制者可以无限期存储和使用数据。

专门为这些目的处理个人数据的数据控制者可以出版发表所取得的成果和分析，并事先采取必要措施对发布的数据进行匿名化处理。

第十六条之六 地理位置数据。数据主体的个人地理位置数据的处理可以基于本法第十二条和第十三条规定的相同法定来源进行。

数据主体必须以清晰、充分和及时的方式被告知将被处理的地理位置数据的类型、处理的目的和持续时间，以及数据是否会被传输或转让给第三方以提供增值服务。

第三章

与经济、金融、银行或商业义务相关的个人数据的使用

第十七条 负责个人数据登记或数据库的责任主体只能传输与经济、金融、银行或商业的义务相关的信息，前提是这些信息记录在承兑汇票和本票上，或因资金不足、关联的活期账户已关闭或其他原因而被拒绝的支票中；以及不遵守与银行、金融公司、互助抵押管理机构、储蓄和信用合作社、公共机构和受一般法律约束的国有企业以及信贷管理公司间因购买商品房而发生的互助抵押和贷款或信贷义务。与国家农牧发展研究所授予其用户信用有关的信息以及已经重新起草、重新指定或更新的或悬而未决的与经济、金融、银行或商业性质的义务有关的信息除外。

共和国总统通过最高法令确定，通过付款或信贷工具支持的有效签发，其中记录有债务人明确同意或有义务缴纳，以及到期日的其他金钱义务信息，均允许传输。但下列情形的债务信息不得传输：与提供电力、水、电话和煤气服务的公共或私人公司的债务；根据第18591号和第19287号法律与高等教育机构的债务，根据第20027号法律与银行或金融机构的债务，接受由生产促进局管理的高等教育助学贷款或为了自己或第三方接受任何级别的正规教育服务而形成的任何债务；在门诊、医院或紧急医疗保健或行动的框架内，与公共或私人医疗服务提供者和相关公司（无论是金融机构、商业机构或其他类似机构）因为咨询、手续、检查、疗程、手术或护理发生的债务；与高速公路特许经营商因使用其基础设施发生的债务。

管理个人数据库的责任主体不得发布或传输本条中提及的信息，特别是债务人在失业期间的拒付和欠款信息。

为此，失业基金管理局仅可以在受益人的权益存续期间将其数据以商业信息公告（BIC）的形式传达，以阻止此类人员信息的进一步披露。

但是，不在失业保险范围中的人员必须通过商业信息公告（BIC）证明上述条件，并附上合法做出的劳动合同终止结算；如果存在争议的，可出具在劳动监察局的出庭记录，申请此权利有效时间为三个月，最多可延期一次。为了使其续期生效，必须附上债务人的宣誓书，声明其在失业状态。

冻结数据对债务人是免费的。

在雇佣关系终止日期前一年内在商业信息系统中记录的人员数据不会被冻结。

责任主体必须从其登记册或数据库中删除与规定义务相关的所有个人信息，而无需请求、法院命令或数据保护机构的指示。

负责管理个人数据库的责任主体在任何情况下都不得以任何形式声明相关人员受益于本法。

第十八条 自相关义务生效起五年内，在任何情况下都不得传播与已识别或可识别的个人相关的前一条提及的数据。

清偿或通过其他合法手段解除债务后，与上述义务相关的数据亦不能继续传播。

但是，法院有权被告知未决诉讼所需的相关信息。

第十九条 为本法第四条的目的，以任何其他方式清偿或解除的债务不会导致相关数据的法律依据的失效或丧失，而前一条规定的条款尚未确定。

通过债权人直接干预的其他方式偿清或解除债务的，债权人应在不迟于随后的七个工作日内将这一事实通知公众可访问的数据库，更新兑付或拖欠信息。为了更新相应数据，债务人需先缴纳相关费用（如果适用）。债务人可以向债权人提供充分付款证明，以申请直接修改数据库并免除债务；所有决定必须以书面形式明确表达。

负责收集或处理公共平台个人数据的责任主体在收到债务清偿或解除通知后，须立即或在随后三天内以相同的方式修改更新数据。若无法修改的，需要冻结数据主体的相应数据，直到信息更新完毕为止。

违反任何上述义务的，将根据本法第七章的规定予以通报和处罚。

第四章

公共机构对个人数据的处理

第二十条 公共机构处理数据的一般规定。公共机构在其职权范围内根据法律规定和本章条款，为履行其法定职能而进行的个人数据处理活动是合法的。在这种情况下，公共机构作为数据控制者，不需要取得数据主体的同意来处理其个人数据。

第二十一条 公共机构处理数据的原则和规定。公共机构对个人数据的处理需遵守本法第三条规定的原则和国家行政机关的一般原则，特别是合作、廉洁和效率原则。

遵照合作原则，公共机构间必须实现高度的互操作性和连贯性，以避免存储信息矛盾和重复向数据主体索取资料或文件。根据效率原则，必须避免公共机构间以及公共机构与数据主体之间的程序和手续重复。

在不影响本章规定的其他条款的情况下，本法第二条、第十四条、第十四条之二、之三、之四、之五、之六和第十五条之二、第二章第二节和第三节以及第五章和第七章的条款的规定适用于公共机构进行的数据处理，同样，根据本法第二十三条的规定，本法第四条、第五条、第六条、第七条和第八条也适用于公共机构进行的数据处理。

第二十二条 公共机构数据传输或转让。为履行法定律职能，在其职权范围内公共机构有权将特定的个人数据或全部或部分数据库或数据集传输或转让给其他公共机构。数据的传输或转让必须针对特定处理目的，接收公共机构不得将其用于其他目的。

为了向数据主体提供便利，避免行政程序重复或向同一数据主体重复索取资料或文件，公共机构之间也可以传输或转让个人数据或数据库。

接收数据的公共机构只能在执行特定处理所必需的时间内保留数据，之后必须将其删除或匿名化。公共机构需要处理申诉或抗议、开展控制或监测活动或用于保证裁决的，这些数据可以存储更长时间。

公共机构必须取得数据主体的同意才能将个人数据传输或转让给个人或私人实体，履行公共机构监检职能所必须的数据传输或转让除外。

根据第20285号法律第十条规定的信息访问请求需要传输或转让个人数据时，公共机构应根据本法第二十条规定取得数据主体的同意。

与刑事、民事、行政和纪律违法违规行为有关的数据传输，适用本法第二十五条规定。

公共机构必须每月通过其机构网站通报与其他公共机构和私人实体签署的有关个人数据转让或转移的协议。该义务由监管机构监督。

第二十三条 行使数据主体权利的行政监督和诉讼程序。数据主体向公共机构行使本法规定的知情权、更正权和异议权。数据主体也可以反对违反本章规定的特殊数据处理。前条第三款规定的情形下，数据主体可以行使删除权。

有下列情形之一的，公共机构不接受访问、更正、反对、删除或临时冻结个人数据的请求：

（一）妨碍或阻碍公共机构履行监督、调查、保护受害者和保护证人以及处罚职能。

（二）影响法定的信息机密性。

数据主体权利的行使必须依照本法第十一条规定的程序进行，向公共机构领导提出。

公共机构明示或默示拒绝行使本法规定的任何权利的请求的，数据主体可以向该机构提出诉讼。诉讼必须遵循本法第四十一条维权行政程序的规定。

第二十四条 特别制度。有下列情形之一的，相关公共机构进行个人数据的处理、传输或转让必须遵循本条特别规章制度的规定：

（一）为预防、调查、侦查或起诉刑事犯罪或执行刑事处罚而进行的活动，包括保护和预防危害公共安全威胁和风险的活动，以及为保护受害者和证人的有关活动。

（二）直接关系国家安全、国防和外交政策的。

（三）依法宣布并且仅在宣布有效期间，为应对紧急情况或灾难为唯一目的而进行的活动。

（四）受有关法律的保留保密规定保护的。公共机构根据法律义务必须转让数据到其他公共机构或第三方的，接收方必须在处理这些数据的同时遵守相同的保留保密义务。

相关公共机构在其职权范围内，可以依照《智利共和国政治宪法》第十九条第四款规定的根本保障以及本法第三条规定的原则以合法方式处理、转让和传输个人数据以履行其法定职能。

为了执行上述第一、二、三项情形的个人数据处理、转让和传输，公共机构及其当局有义务交换信息并提供情形所需的个人数据，前提是这些处理活动为法律规定的特定目的而进行，如无法做到，则必须要有必要的和相对应的措施。

个人数据保护监管局可以在听取相应主管机构的意见后下发指示，明确如何将上述保障和原则应用于上述情形，以确保其受到保护并允许有效履行相应机构的法定职能。

第二十五条 与刑事、民事、行政和纪律违法违规有关的数据。与刑事、民事、行政和纪律违法违规行为的实施和处罚相关的个人数据只能由公共机构在其职权范围内并在法律明确规定的情况下为履行其法定职能而处理。

公共机构之间的沟通涉及处理这些个人数据的，必须始终确保传达或公开的信息是准确、充分、最新且完整的。

一旦规定了相应的刑事、民事、行政或纪律处分，或者一旦执行或规定了处罚，且由主管公共当局宣布或核实，则不得传达或公开与刑事、民事、行政或纪律违法违规行为的实施和处罚有关的个人数据。上述规定不影响按照规定相应具体义务的法律规定的方式和时间，依法在公共机构保存的记录中纳入、维护和查询这些信息。公共机构的公职人员有义务对这些信息进行保密并作为保留信息保存。

当法律规定与刑事、民事、行政和纪律违法违规行为的实施和处罚有关的信息必须通过将其纳入处罚登记册或在公共机构网站上或以任何其他交流和传播方式发布，而没有规定信息保留期限的，将遵循下列规则：

（一）刑事犯罪，公示期受相应违法事件的特定法规约束。

（二）民事、行政和纪律违法违规行为，五年内向公众公开。

禁止对公共机构保存刑事、民事、行政和纪律违法违规行为的电子记录中的个人数据进行大规模处理。根据本法，不遵守该禁令则构成极其严重的违法违规行为。

法院或其他公共机构为履行其法律职能并在其职权范围内要求提供信息的情况不受禁止交流的限制，但要确保数据适当的保密性。

尽管有本条第三款的规定，与刑事犯罪实施和处罚有关的个人数据将予以保留，除法律另有规定的，持有公共机构不得传输或转让这些数据给第三方。

第二十六条 条例。公共机构之间以及与私人或公共机构之间的个人数据传输或转让的条件、方式和工具根据个人数据保护监管局的报告，经财政部长和经济、发展和旅游部长联合签署，由总统府秘书处颁布的条例来规定。同样的条例适用于规范个人数据的匿名化程序，尤其是敏感个人数据。

本条例不适用于本法第八章提及的机构参与的任何数据转让处理。

第五章

个人数据跨境传输

第二十七条 一般规定。一旦满足本法关于授权处理数据的要求，有下列情形之一的，数据跨境传输都是合法的：

（一）根据第二十八条的规定，向个人、实体或公共或私人组织传输数据的，受制于对个人数据提供足够保护水平的国家的法律制度。

（二）数据传输包含在数据控制者与接收者或第三方代理人之间签署的合同条款或其他法律文书中，且已明确数据主体的权利和保障，相关责任人和第三方的义务以及控制方式。

（三）数据控制者和接收责任人，包括第三方接收代理人，根据各自适用的法律，采用具有约束力和经过认证的合规模式或自我调节模型。

（四）数据主体明确同意进行特定且确定的个人数据跨境传输的。

（五）涉及特定的银行、金融或股票，根据相关法律规范进行的数据传输的。

（六）按《证券市场法》规定的属于同一企业集团、关联公司或同一控制人的公司或实体之间进行数据传输的，前提是所有这些公司或实体在个人数据处理方面都遵循相同的标准和政策。数据控制者必须对企业集团某些人员违反具有约束力的相关企业标准和政策的行为承担责任。数据控制者只有证明违规行为与相应企业成员无关时，方可免除责任。

（七）为了遵守智利国家批准且有效的国际条约或协议中规定的义务而必须传输数据的。

（八）为了满足公共机构因履行和行使其职能和权力而签署的合作协议、信息交流或监督而必须进行数据传输的。

（九）自然人、公法人或私法人已获得法律明确授权并出于特定目的而进行数据传输的。

（十）以提供或请求国际司法合作为目的而进行数据传输的。

（十一）为了签订或执行数据主体与相关责任人之间的合同，或因数据主体要求执行合同前措施而需要进行数据传输的。

（十二）因预防或诊断疾病、医疗、卫生服务或健康管理需要在医疗或卫生方面采取紧急措施的。

第二十八条 确定国际数据传输的适用国家及其他规则。当一个国家或地区的法律体系达到与本法规定的标准相似或更高的标准时，它就具有足够的数据保护水平。为了合理确定具有足够数据保护水平的国家或地区，监管机构将至少考虑下列因素：

（一）制定管理个人数据处理的原则。

（二）具有认可和保障数据主体权利的法规，且具有控制或监护职能的司法或行政公共权力机构。

（三）对数据控制者及第三方规定强制性的信息安全义务。

（四）违法行为的责任认定。

监管机构将在其网站上向各方提供一份适用国家名单和合同条款的标准模型，以及数据跨境传输的其他法律文书。

上条所述情况均未得到证实时，监管机构可以通过合理的决议授权在特定情况下进行数据跨境传输，前提是数据的发送者和接收者可以根据本法就数据主体的权利和传输信息的安全性提供充分保证。充分保证将被视为那些包含与本法提供的原则、权利和保证类似或更多的文书、机制和条款，特别是授予数据主体可执行权利和有效法律行动的文书、机制和条款。为了进行数据传输验证，监管机构会施加一些先决条件，并会批准包含上述数据跨境传输的保障性示范条款，这些条款将提供给相关责任人。

跨境传输数据控制者必须向监管机构证明进行的数据传输遵守本法规定的规则。

第二十九条 监测。监管机构负责监测数据跨境传输操作，可以提供建议，采取保守措施，并在符合条件的情况下暂时中止数据发送。

第六章

个人数据保护监管机构

第三十条 个人数据保护监管局。个人数据保护监管局是一家公法自治机构，具有技术性、去中心化的特点，具有法人资格和自有资产，并通过智利经济、发展和旅游部与共和国总统联系。

监管机构的宗旨是根据本法规定确保个人隐私和数据得以有效保护，并监督本法落实情况。

监管机构的法定地址将在法律条例中明确规定，但并不妨碍其在智利其他地区设立分址。

第三十条之二 监管机构的职能和权力。监管机构具有下列职能和权力：

（一）为规范个人数据处理的操作，根据本法规定的原则，发布一般性和强制性的指示和规则。一般性指示和规则必须与严格遵守本法的个人数据处理的规定严格相关，包含方便各利益相关方提出意见的必要机制，并通过其网站公开征求意见后发布。

（二）在行政上适用和解释关于个人数据保护的法律法规及监管机构发布的一般性指示和规则。

（三）监督关于个人数据处理的本法规定、条例及发布的一般性指示和规则的落实情况。为此，监管机构可要求个人数据处理者提供任何可能形式的文件、记录或材料，以及履行其监督职能所需的所有相关信息。

（四）确定个人数据处理者在数据处理操作过程中违反本法所规定的原则和义务、条例以及监管机构发布的一般性指示和规则的行为。为此目的，在充分理由依据下，为了执行处罚程序，监管机构可以传唤包括数据主体、法定代表人、管理人、顾问、雇员以及参与或了解相关事实的任何人员。监管机构也可以通过其他方式来确保各自陈述的真实性。

（五）根据本法规定的处罚形式，行使权力处罚违反本法律法规以及监管机构发布的一般性指示和规则的处理个人数据的自然人或法人。

（六）解决数据主体对违反本法律法规或监管机构发布的一般性指示和规则的个人数据处理者提出的请求和诉讼。

（七）制定方案、项目和行动，向公众传播、宣传和提供关于个人数据保护的相关信息。

（八）酌情向共和国总统和国会提出法律法规规则建议，以确保个人数据得到应有的保护，并完善信息处理和使用的相关规定。

（九）在必要时向国会、司法部、共和国总审计署、检察院、宪法法院、中央银行、选举事务机关、司法选举机关和其他依法设立的特别法庭在制定和实施其内部政策和规则方面提供技术援助，以便其个人数据处理的操作和活动按照本法规定的原则和义务进行。

（十）与公共机构建立联系并合作，设计和实施旨在确保个人数据保护和正确处理的政策和行动。

（十一）与具有相关职能或个人数据领域的国内外公共或私营实体签署合作和协作协议。在与国际公共机构签订协议时，应根据第21080号法律第三十五条的规定事先与外交部进行协商。

（十二）参与并与国际机构合作与协作个人数据保护事务。

（十三）认证、登记和监督预防违规模型及合规方案，管理国家处罚与合规登记册。

（十四）行使法律赋予的其他职能和权力。

如果行政机构行使本法赋予监管机构的职能或权力，则必须遵守第19880号法律第十四条第二款的规定。

第三十条之三 监管机构的管理。监管机构的管理委员会为高级管理层，其职能和权力如下：

（一）行使法律赋予的权力和履行法律赋予的职能。

（二）为履行法律赋予的职能，制定监管机构运作的内部规章制度。

（三）制定监管机构运作的规划、组织、管理、监督、协调和控制政策，以及资产管理、获取和处置政策。

（四）发布一般性条例、通函、公告和其他必要的决议。

（五）向共和国总统或国会提出相关法律法规规则的修改建议。

（六）在每年的前四个月内，编制一份公共年度账目，详细说明监管机构在上一年度所开展的工作。

第三十条之四 监管机构管理委员会成员。监管机构管理委员会由三名顾问组成，征得参议院三分之二的在职议员的同意后由共和国总统任命。

共和国总统提出管理委员任命候选名单，参议院应就该提议投票作出决定。

管理委员候选人必须是在个人数据保护方面具有公认的专业或学术声望的人。

管理委员会应根据监管机构章程的规定，从其成员中任命主席和副主席。主席和副主席的任期为三年，或在其担任董事的剩余任期。

管理委员的任期为六年，不得连任，每两年单独更新一次。

监管机构的管理委员是专职的。

管理委员会采用多数决原则，如果票数相等，则由其主席或在其主席缺席的情况下由副主席决定。最低法定人数为两名。其他规则的运作需遵守本规定。

管理委员会应至少每周举行一次例会。当主席亲自召集或由两名董事书面要求时，还应该按照其内部规定确定的形式和条件召开特别会议。主席不得拒绝所召集会议的执行，相应的会议应在要求后的两个工作日内举行。

第三十条之五 不适任和不胜任。管理委员不可兼任其他任何私营部门的有偿或无偿职位或服务职责。同样，也不可兼任下列任何情形的职责或职务：政党领导机构成员、政府官员，以及任何由财政资金或市政资金支付的有偿或无偿职务；国内外自治机构、公共或私营实体中的有偿或无偿职务；国有企业和一般情况下依法设立的任何公共服务机构，以及国家、国有企业、中央或地方机构拥有多数资本份额或同等比例或相等比例的代表权或参与权的公共或私营实体；以及其他任何企业或实体的顾问、董事或员工。此外，亦不可兼任国家任何权力机构中任何有偿或无偿的工作或服务职责。

管理委员可兼任国家认可的公立或私立教育机构的教职，每周最多不得超过十二个小时。

管理委员的配偶或有民事关系的伴侣及其直系和二代旁系亲属，不得在从事收集、处理或传输个人数据的公司担任董事职位或拥有股权。

下列人员不能被任命为管理委员：

（一）因渎职罪、行贿罪以及在行使公共职能时犯下的罪行、经济罪和违反公共信任罪被判重罚或终身禁止担任公职的人员。

（二）除医疗目的外，对非法麻醉品或精神药物有依赖的人员。

（三）近五年内严重或极其严重违反规范个人数据处理和保护的规则而受到处罚的人员。

（四）在过去一年内，在从事收集、处理或传输个人数据的公司担任经理、数据保护专员、董事或拥有股权的人。

在本条未明确规定的事项将适用2000年由总统府总秘书处颁布的第1-19653号具有法律效力的法令《重新起草并加以协调与系统化第18575号法律〈国家行政机关组织总法〉》第三章第二节的规范。

第三十条之六 管理委员免职和解职原由。若管理委员能力不足，有不当行为或存在明显赎职行为，总统或众议院可通过简单多数的表决，或由十五名国会议员提出申请并要求最高法院解除其职务。最高法院应就此召开特别会议，并需获得现任成员多数一致同意才能决定解除其管理委员职务。

除免职外，下列情形也是解除管理委员职务的原由：

（一）任期届满。

（二）向共和国总统提出辞职。

（三）参加民选职务竞选。

（四）由除当事人外大多数管理委员评估确定的不适任或不胜任的情形。

如果一名或多名管理委员因任何原因离任，将根据本法第三十条之四规定的相同程序，根据共和国总统的提议，在剩余期限内任命新管理委员。

如果根据本条规定解职的管理委员担任管理委员会主席或副主席，则应按本法第三十条之四规定的方式任命其继任者，任期为离任者任期所剩时间。

第三十条之七 薪酬。管理委员会主席负责行使本法第三十条之九和其他相关法律规定的职能，其总月薪水平和政府司长的薪酬相当。

其他管理委员的薪酬水平相当于管理委员会主席薪酬的百分之八十五。

第三十条之八 监管机构章程。章程规定了监管机构的运作规则。章程及其修改应由监管机构向共和国总统提出，并由经济、发展和旅游部颁布的最高法令予以批准。

第三十条之九 监管机构管理委员会主席的职责和权力。监管机构管理委员会主席是监管机构的负责人，拥有监管机构的司法和法外代表权，负责该机构的组织和行政工作，并负责对机构人员的行动进行分级监督和管理。

管理委员会主席特别拥有下列职能和权力：

（一）行使机构最高领导的职责。

（二）执行并遵守管理委员会通过的规定和协议。

（三）召集和主持管理委员会会议，制定会议议程。

（四）在法律、司法和司法外各层面代表机构。

（五）在机构管理委员会事先同意的情况下，为管理委员会的正常运作颁布必要的内部规章，并确保遵守机构所适用的规则。

（六）根据法律规定，雇佣和解雇机构公职人员。

（七）为实现管理委员会的宗旨，实施必要的行为并签订公约或协议。

（八）授予特定的职责或权力给机构公职人员。

（九）维护本机构与公共机构、其他国家机构、受其监管的个人或实体以及国际个人数据监管机构之间的关系。

（十）履行机构管理委员会授予的其他职责。

在主席缺席时，管理委员会副主席将承担主席的职能和权力。

第三十一条 与信息透明委员会的监管协调。当监管机构根据第20285号法律规定的职能和权力发布可能影响到信息透明委员会主管领域的一般性和强制性指示或规则时，应向其发送所有背景资料，并要求其出具报告，以避免或预防潜在

的规则冲突，并确保双方机构之间的协调、合作和协作。

信息透明委员会必须在收到上述要求后的三十个自然日内提供所要求的报告。

监管机构应在其发布的指示或规则中考虑信息透明委员会关于透明度的意见内容。若逾期未收到报告，应按照第19880号法律第三十八条第二款的规定进行处理。

同样，当信息透明管理委员会必须颁布具有明显影响监管机构职能和权力的一般性指令时，也应发送背景资料并要求监管机构出具报告。监管机构应自收到请求之日起三十个自然日内提交报告。信息透明管理委员会应在其发布的指示或规则中考虑监管机构的意见内容。若逾期未收到报告，应按第19880号法律第三十八条第二款的规定进行处理。

第三十二条 机构人员和监管。在监管机构工作的人员受《劳动法典》的约束。

除此之外，第20880号法律《关于公务廉政和利益冲突预防》和2000年由总统府总秘书处颁布的第1-19653号具有法律效力的法令《重新起草并加以协调与系统化第18575号法律〈国家行政机关组织总法〉》第三章的规定也适用于监管机构的工作人员。这些规定条款必须在与工作人员对应的合同中予以明确。

在监管机构担任管理职务的人员通过国家公务员局开展的公开竞聘从对应职务的三名候选人中产生，三名候选人名单由公共高级领导委员会遵照第19882号法律规定的公共高级领导选拔程序来确定。

如果第三方因管理委员会成员或机构公职人员履行职责时的正式行为或在执行职务时产生的作为或疏忽而对其提起法律诉讼，机构应向他们提供法律辩护。即使在其任职终止之后，且这种辩护可扩展到对他们提出的所有诉讼。

若其正式行为、作为或疏忽已构成公职行为人的解雇原由，则不适用前款所述之辩护。

该机构应遵守1975年第1263号法令《关于国家财政管理法》的各项规定。

该机构还应接受共和国总审计署对其公职人员及其账户的审查和审计的监督。

机构的决议将免受共和国总审计署的审核程序。

第三十二条之二 资产。该机构的资产包括：

（一）《公共部门预算法》中每年规定的拨款。

（二）转让给机构或机构获得的动产和不动产以及其孳息。

（三）机构接受的捐赠。这些捐赠无需进行《民法典》第一千四百零一条规定的司法授权程序。

（四）机构接受的遗产和遗赠应始终为库存收益，且免于各种税收及产权税，或其他因此产生的费用。

（五）国际合作的援助。

第七章

违法行为及其处罚、程序和责任

第三十三条 一般责任制度。数据控制者，无论是自然人、公法人或私法人，如果在其个人数据处理操作中违反了本法第三条规定的原则、本法规定的权利和义务，将依据本章的条款受到处罚。

第一节

适用于自然人或私法人的责任、违法行为和处罚

第三十四条 轻微、严重和极其严重的违法行为。数据控制者违反本法第三条规定的原则、本法规定的权利和义务的行为，根据其严重程度分为轻微、严重和极其严重的违法行为。

自然人或法人因违反本法规定的行为而承担的责任，不影响可能与之相应的

其他法律、民事或刑事责任。

第三十四条之二 轻微违法行为。下列情形视为轻微违法行为：

（一）完全或部分不遵守本法第十四条之三规定的信息透明义务。

（二）缺乏与数据控制者或其法定代表人进行沟通的邮寄地址、电子邮件地址或等效电子媒介，该信息必须保持更新和有效，以便数据主体可以进行通信或行使相应权利。

（三）未回应、部分回应或超期回应数据主体根据本法提出的请求。

（四）未向监管机构提交本法或其条例强制规定的呈报文件。

（五）未遵守监管机构发布的一般性指示，但不视为严重或极其严重的违法行为。

（六）在预防违法模型的登记或认证过程中提供不完整的信息。

（七）违反本法规定的权利和义务的其他任何违法行为，但不视为严重或极其严重的违法行为。

第三十四条之三 严重违法行为。下列情形视为严重违法行为：

（一）未经数据主体同意或在无法律先例或法律依据的情况下处理个人数据，或将其用于与其收集目的不同的其他目的。

（二）必须取得数据主体同意的，没有取得数据主体同意，交流或转让个人数据，或为授权以外的目的交流或转让数据。

（三）违反本法第三条第三项规定的原则，处理与处理目的不必要的个人数据。

（四）处理与处理目的相关的不准确、不完整或未更新的个人数据，法律或合同规定数据主体具有更新责任的除外。

（五）阻碍或妨碍数据主体依法行使知情权、更正权、删除权、异议权或携带权。

（六）数据主体有正当理由请求暂停处理个人数据的，未回应、过时回应或无正当理由拒绝请求。

（七）违反本法规定处理儿童和青少年的个人数据。

（八）非营利私法人不符合用于政治、哲学、宗教、文化、工会或行业协会目的的个人数据处理规定的要求，处理其员工的数据。

（九）违反本法第十四条之二规定的保密义务。

（十）违反本法第十四条之五规定的处理个人数据的安全义务。

（十一）未报告或未记录违反本法第十四条之五规定的安全措施的情况。

（十二）出于历史、统计或科研目的以及用于为公共利益服务的研究调查，个人数据的处理所采取的质量安全保证措施不充分或不适当。

（十三）违反本法跨境数据传输规定进行跨境数据传输操作。

（十四）未遵守监管机构发布的直接具体的决议或要求。

第三十四条之四 极其严重的违法行为。下列情形视为极其严重违法行为：

（一）以欺诈方式处理个人数据。

（二）恶意分配个人数据用于数据主体同意的或法律准许以外的目的。

（三）故意传播或披露有关数据主体不真实、不完整、不准确或未更新的信息。

（四）违反对敏感个人数据和与刑事、民事、行政和纪律违法行为的实施和惩罚有关的个人数据的保密义务。

（五）违反本法规定，故意处理、传播或转让敏感个人数据或儿童和青少年的个人数据。

（六）故意不报告可能影响个人数据的保密性、可用性或完整性的违反安全措施的行为。

（七）未经法律授权，对公共机构保存的刑事、民事、行政和纪律违法行为的电子记录中的个人数据进行大规模处理。

（八）故意违反本法规定，进行跨境数据传输操作。

（九）违反监管机构处理数据主体对行使其知情权、更正权、删除权、异议

权、携带权或冻结权的诉讼的决议。

（十）在预防违法模型的登记或认证过程中故意提供虚假、不完整或明显错误的信息。

（十一）在相应情形下，未遵守本法第十五条之三规定的义务。

第三十五条 处罚。对数据控制者的违法行为的处罚如下：

（一）轻微的违法行为将受到书面警告或处以最高一百个月税单位（UTM）的罚款。

（二）严重的违法行为将被处以最高五千个月税单位（UTM）的罚款，违法者是企业的，则将被处以最高相当于上一自然年销售和服务及其他业务活动年收入百分之二的罚款，最高为一万个月税单位（UTM）。

（三）极其严重的违法行为将被处以最高一万个月税单位（UTM）的罚款，违法者是企业的，则将被处以最高相当于上一自然年销售和服务及其他业务活动年收入百分之四的罚款，最高为两万个月税单位（UTM）。

监管机构必须针对每个案件指明补救措施，旨在纠正引起处罚的原因，这些补救措施必须在不超过六十天的期限内执行，否则将对所处罚款加收百分之五十的附加费，但不影响本法第四十九条的规定。如果再犯，根据本法第三十六条第二款第一项的规定，监管机构可处以高达所犯罪行金额三倍的罚款。

第三十六条 责任减轻和加重情节。下列情形视为减轻情节：

（一）数据控制者采取的单方面补救措施以及与受影响的数据主体达成的赔偿协议。

（二）违法者在监管机构进行的行政调查中提供的配合。

（三）数据控制者之前没有被处罚的记录。

（四）向监管机构主动汇报。同时，违法者必须视情况通报为制止导致违法行为的事件而采取的措施或实施的缓解措施。

（五）认真履行对处理的个人数据保护的管理和监督职责，并依照本法第五十一条的规定出具证明予以核实。

下列情形视为加重情节：

（一）累犯。数据控制者在过去三十个月内因违反本法而受到两次或多次处罚的，即为累犯。适用相应处罚的决议必须是具有强制力的。

（二）违法行为的持续性。

（三）危及与其个人数据相关的数据主体的权利和自由的安全。

第三十七条 罚款额的确定。为了确定本法规定的罚款额，监管机构应审慎适用下列标准：

（一）行为严重程度。

（二）失职或疏忽是否为导致违法行为的原因。

（三）违法行为造成的损害，特别是受影响的数据主体的数量。

（四）因违法行为而获得的经济利益（如有）。

（五）所进行的处理是否包括敏感个人数据或儿童和青少年的个人数据。

（六）违法者的经济能力。

（七）监管机构先前在相同情况下实施的处罚。

（八）发生的减轻和加重情节。

如果一次行为导致两项或多项违法，或者当一项违法是实施另一项违法的手段时，应只处以一次罚款，并始终考虑最严重违法的严重程度。经核实存在两项或多项彼此独立的违法行为的，每一项违法对应的处罚都应累加。

罚款必须在监管机构的决议生效之日起十个工作日内当面或以可用的电子支付方式缴纳给国库。相应的付款凭证应在付款之日起十个工作日内提交给监管机构。

第三十八条 附加处罚。在二十四个月内因屡次极其严重违法而被处以罚款，监管机构可以下令中止数据控制者进行的数据处理操作和活动，最长期限为三十天。这种中止不会影响数据控制者对数据的存储。

作为附加处罚，监管机构命令的中止可以是针对部分或全部数据，在影响到数据主体的权利时，不得命令中止。

在中止期间，数据控制者必须采取必要措施，使其业务和活动符合中止命令

决议中规定的要求。

若数据控制者不遵守临时中止决议的规定，该措施可无限期延长，每次最长连续三十天，直到数据控制者遵守中止命令为止。

中止影响到受公共监督机构监督的实体的，监管机构必须事先将事实告知相关监督机构，以保护该实体用户的权利。

第三十九条 国家处罚与合规登记册。国家处罚与合规登记册由个人数据保护监管局来管理。该登记册是公开的，可免费访问的，并以电子形式查阅和运营。

登记册必须记录因违反本法规定的权利和义务而受到处罚的数据控制者，并根据违法行为的严重程度进行区分，同时记录违法行为、责任减轻和加重情节以及所实施的处罚。具有有效资质的采用经认证的预防违法模型的数据控制者也应当备案。

登记册中的记录信息应在登记之日起五年内可公开查阅。

第四十条 诉讼时效。对本法规定的违法行为的诉讼时效期限为四年，自违法行为发生之日起计算。

持续违法的，违法行为的诉讼时效期从违法行为停止之日开始计算。

一旦启动行政程序，诉讼时效即告中断。

因违反本法规定而被处以处罚的时效期限为三年，自处罚决议执行之日起计算。

第二节

行政程序

第四十一条 维权行政程序。数据控制者拒绝依照本法第十一条所提出的请求，或在规定的法定期限内未回应请求的，数据主体可以向监管机构提出行政诉讼。

提出诉讼必须依照下列规则：

（一）在收到数据控制者拒绝回应的十五个工作日内或数据控制者回应数据主体提出的请求但已逾期的，数据主体必须以物理或电子方式的书面形式提出诉讼。诉讼应明确提出对请求被拒绝或无回应的异议并附上所有证据，以及提供邮寄地址、电子邮件地址或其他等效电子媒介以便接收通知。

（二）在提出诉讼时，应数据主体充分理由的要求，仅在合理的情况下，监管机构可以在事先听取数据控制者的意见后，临时叫停处理有关提出诉讼的数据主体的个人数据。

（三）收到诉讼后，监管机构必须在十个工作日内确定诉讼是否满足前项规定的受理要求。诉讼不予受理的，监管机构所做出的决议必须依据充分，并通知到数据主体。在任何情况下，监管机构在上述期限内未作出决定的，视为诉讼被受理。

（四）一旦诉讼予以受理，监管机构将通知数据控制者，数据控制者必须在十五个工作日内对诉讼作出回应，并附上其认为相关的所有背景资料。给数据控制者的通知应发送至其邮寄地址、电子邮件地址或本法第十四条之三第三项提及的其他等效的电子媒介。

（五）期限届满后，无论数据控制者是否作出回应，只有在存在实质性、相关和有争议的事实时，监管机构才可以开展为期十个工作日的举证期，期间双方都可以提交所有认为适当的证据。

（六）数据控制者在其回应中可以接受诉讼，在这种情况下，必须提供证明这种情况的记录或证据。一旦情况得到核实，数据主体将收到通知，并有十天的时间来行使自己的权利。一旦期限届满，监管机构在必要时对数据控制者加以处罚亦或给予指示，并对记录进行归档。

（七）监管机构拥有广泛的权力，以要求提供有助于其决议的背景资料或报告，可以召集双方参加听证会并敦促达成协议。若未达成协议的，监管机构的公务员在听证会上可能发表的意见不影响其继续审理该案件的资格。一旦达成协议，记录将被归档。

（八）监管机构作出的诉讼决议必须依据充分。维权行政程序不得超过六个月。

（九）对于监管机构不受理诉讼的决议和解决诉讼的决议，可在通知后的十五个工作日内，依照本法第四十三条规定的程序向法院提出申诉。

在临时冻结请求被拒绝的情况下提出的诉讼和暂停处理的请求，监管机构应在最多三个工作日内作出决定，且无需事先听取各方意见。

第四十二条 违法行政诉讼。数据控制者因不遵守或违反本法第三条规定的原则、本法规定的权利和义务而引起的违法行为的认定以及相应处罚的考量，应遵循下列特别规则：

（一）处罚程序由监管机构指示。

（二）审计完成或数据主体提出诉讼后，监管机构可依职权或应一方要求，根据本法第二十三条和第四十一条规定的程序启动处罚程序。在后一种情况下，监管机构必须证明已收到诉讼请求。立案同时，监管机构必须指定一名负责审理案件的公务员。

（三）监管机构必须提供一份针对数据控制者的指控声明，其中描述构成违法行为的事实、数据控制者违背或违反的原则和义务、违反的法律规则以及任何有助于起诉的其他背景信息。

（四）指控声明必须通过本法第十四条之三第三项指明的邮寄地址，电子邮件地址或其他电子媒介通知到数据控制者。

（五）数据控制者应在十五个工作日内提出抗辩。届时，数据控制者可以附上其认为相关的背景信息以反对指控。连同反驳内容一起，数据控制者应指定一个电子邮件地址用来接收所有其他来文和通知。

（六）收到辩护或辩护期限届满之后，如存在实质性、相关和有争议的事实监管机构可以展开为期十天的举证期。

（七）监管机构应允许数据控制者在其辩护中要求采取的任何相关且必要的措施或取证程序。若拒绝，应说明理由。

（八）所调查事件和被指控的违法者的责任可用以任何合法的证据手段来指证，其证据评估遵从合理批评的规则。

（九）监管机构拥有广泛的权力，以要求提供有助于其决议的背景资料或报告。

（十）行政裁决必须依据充分，并解决案件中提出的所有问题，对数据控制者提出的每一项指控和辩护作出裁决，包含数据控制者不遵守或违反法律规定的原则、权利和义务的声明或视情况宣告无罪。如果监管机构认为违法行为已被证实，将在同一决议权衡加重或减轻违法者责任的情节，并根据所犯违法行为的严重程度给予处罚。

（十一）确定不遵守或违反本法的原则、权利和义务并适用相应处罚的决议必须依据充分。该决议必须说明根据本法可以对其提出行政和司法上诉，并必须指明上诉机构以及提出上诉的期限。可根据下一条规定对监管机构关于违法行为的决议进行司法诉讼。

（十二）违法行为的行政诉讼不得超过六个月。自本条第二项所述的证明之日起超过六个月，监管机构仍未解决诉讼的，当事人可以根据下一条规定提出不法上诉。

第三节

司法上诉程序

第四十三条 司法上诉程序。相关自然人或法人如果认为阻碍程序的行政行为或监管机构做出的终裁是非法的，可以向圣地亚哥上诉法院或上诉人居住地的上诉法院提出不法上诉，由上诉人自行选择。上诉必须在收到有争议的裁决通知后的十五个工作日内，根据下列规则提出：

（一）上诉人在上诉书中应准确说明作为上诉对象的裁决、被认为违反的法律规则、违反的方式，以及在必要时，该行为所造成伤害的原因。

（二）如果上诉书未满足前项所述条件，则上诉法院可以宣布诉讼不予受理。此外，当有争议行为的实施对上诉人造成无法挽回的损害时，上诉法院可以下令停止执行受争议的裁决。

（三）收到上诉后，上诉法院将要求监管机构在十天期限内出具报告。

（四）一旦收到报告或缺省少报告的，法院认为有必要的，可以依照《民事诉讼法典》的相关规定展开举证期。

（五）举证期限届满后，案件将提交法院审理。案件可优先纳入审理日程。

（六）法院审理上诉的，应在判决中判断是否存在错误，必要时责令纠正有争议的行为并发布相应的判决。

（七）对于违反处罚程序的决定的上诉，法院可以维持或撤销有争议的决定，酌情确定或驳回违法行为，并视情况维持、撤销或修改对数据控制者的处罚或宣告无罪。

（八）本条未规定之情形，将酌情适用《法院组织法》和《民事诉讼法典》中规定的条款。

第四节

公共机构、机构当局或领导人及公职人员的责任

第四十四条 公共机构领导人的管理责任。公共机构领导人应确保各机构根据本法第四章规定的原则、权利和义务开展其个人数据处理业务和活动。

此外，公共机构应遵守监管机构提出的旨在补救或防止违法行为的措施或本法第四十九条规定的合规或预防违法方案。

对于本法第三十四条之二、之三和之四界定的公共机构违反本法第三条规定的原则以及本法规定的权利和义务的违法行为，违法的公共机构领导人将被处以月薪百分之二十至五十的罚款。罚款额的确定应考虑到违法的严重程度、所处理数据的性质和受影响的数据主体的数量并权衡责任减轻和加重情节。

公共机构继续违法的，公共机构领导人将被加倍处罚并停职五天。

涉及敏感个人数据的，违法公共机构领导人将被处以月薪百分之五十的罚款并停职最多三十天。

公共机构在处理个人数据过程中发生的违法行为将由监管机构根据本法第四十二条规定的程序来确定。

违法行为一旦确定，监管机构应实施本条规定的行政处罚。共和国总审计署可应监管机构要求，根据其组织法的规定，启动行政程序并提出相应的处罚措

施。

可根据本法第四十三条对监管机构的决议提出不法上诉。

本条规定的处罚措施必须在相关决议成为终裁之日起五个工作日内在监管机构和相关机构或部门的网站上公布。

第四十五条 违法公职人员的责任。在不违反前条规定的情况下，如果在相应的行政程序中确定公共机构的一名或多名公职人员存在个人责任，共和国总审计署应根据监管机构的要求启动简易调查，以确定上述官员的责任，或视情况在已经启动的行政程序中进行调查。对违法公职人员的处罚应根据《行政规约》的规定来确定。

如果相应的行政程序证实相关公职人员应对本法第三十四条之四所规定的任何极其严重的违法行为负责，则该行为将被视为严重违反行政廉洁。

第四十六条 公职人员保密义务。处理个人数据的公共机构公职人员，特别是处理涉及敏感个人数据或与刑事、民事、行政和纪律违法违规行为的实施和处罚有关的数据时，必须对其在行使职责时接触的信息进行保密，并避免将这些信息用于与其公共机构的法定职能不相符的目的，或将其用于其个人利益或第三方的利益。根据《行政规约》第一百二十五条第二款的规定，构成违反该规定的事实应被视为严重违反行政廉洁原则，且不影响可能适用的其他处罚和责任。

当公共机构履行法律义务向其他公共机构交流或转让受保密规则保护的数据时，接收公共机构及其公职人员必须对其数据履行同样的保密义务。

第五节

民事责任

第四十七条 一般性规定。当数据控制者在其数据处理操作中违反本法第三条规定的原则、本法规定的权利和义务并导致数据主体受到损害时，数据控制者必须赔偿对数据主体造成的经济和非经济损失。上述规定不妨碍数据主体行使本法所赋予的其他权利。

一旦监管机构做出利于诉讼的决议，或者终审判决正式生效，就可提出前款

所述的赔偿行为。有不法上诉的，将根据《民事诉讼法典》第六百八十条及其后续条款规定的简易程序处理。

因违反本法而引起的民事诉讼，诉讼时效为五年，自行政决议或法院判决执行之日起起算，视情况处以相应的罚款。

第四十八条 预防违法。数据控制者，无论是自然人、公法人或私法人，都应采取行动防止发生本法第三十四条之一、之二和之三条确定的违法行为。

第四十九条 预防违法模型。数据控制者可以自愿制定包括合规方案的预防违法模型。

合规方案应至少包含下列要素：

（一）任命数据保护专员。

（二）定义数据保护专员的职责和权力。

（三）确定该实体处理的信息类型、地域管辖范围、管理的数据或数据库的类别、级别或类型以及数据主体的特征。

（四）定期或不定期识别实体产生或增加本法第三十四条之二、之三和之四中规定的违法行为风险的活动或流程。

（五）制定具体的协议、规则和程序，使参与前项所述活动或流程的人员能够以防止发生上述违法行为的方式安排和执行其任务或工作。

（六）遵守本法规定的内部报告机制，以及在本法第十四条之六规定的情况下向数据保护机构的报告机制。

（七）具有内部行政处罚规定以及对违反预防违法系统的责任人投诉或处罚的程序。

如适用，因实施合规方案而产生的内部规定作为在充当数据控制者的实体或处理数据第三方的包括高层在内的所有员工、雇员和服务提供者的劳动或服务合同中的义务，或者作为《劳动法典》第一百五十三条及后续条款的规定的内部规定的义务，必须予以明确。在后一种情况下，必须执行《劳动法典》第一百五十六条规定的宣传措施。

第五十条 数据保护专员的职权范围。数据控制者可以任命一名数据保护专员。

数据保护专员应由数据控制者的最高管理层或行政管理当局任命。董事会、管理合伙人或企业或服务部门（视情况而定）的最高权利机构视为最高管理层或行政管理当局。

在与本法有关的事项上，数据保护专员必须具有管理自主权。中小微型企业所有者或其最高领导可以亲自担任个人数据保护专员。

数据保护专员可以执行其他职能和职责，力求保持其职能的独立性。数据控制者必须保证这些职能和职责不会引起利益冲突。

按《证券市场法》规定的属于同一企业集团、关联公司或同一控制人的公司或实体可以任命一名数据保护专员，前提是所有这些公司或实体在个人数据处理方面都遵循相同的标准和政策，且该代表对所有实体和机构都是可及的。

数据保护专员必须由具备担任其职责所需的资质、能力和专业知识的人员担任。

数据主体可以就与处理其个人数据和行使本法规定的权利有关的所有事宜联系数据保护专员。

数据保护专员有义务对其在履行职责时接触到的个人数据严格保密。履行这些职能并违反保密义务的公职人员将根据《刑法典》第二百四十六至二百四十七条之二的规定受到处罚。数据控制者应对其数据保护专员违反保密义务的行为承担责任，但不影响对其可能提起的赔偿诉讼。

数据控制者必须确保数据保护代表官拥有足够的资源和权力来履行其职能，结合公司规模和经济实力，必须提供必要的物质资源以确保其充分开展工作。

在不影响可能分配的其他职能的情况下，数据保护专员应具有下列职责：

（一）告知并建议数据控制者、第三方数据处理者或数据控制者的代理人和雇员有关个人数据保护权及其处理规定的法律和法规规定。

（二）推动并参与数据控制者有关保护和处理个人数据的政策制定。

（三）在其职权范围内监督本法和数据控制者发布的政策的遵守情况。

（四）关注参与数据处理业务的人员的持续培训。

（五）协助组织成员识别与处理活动相关的风险，并采取措施保护数据主体的权利。

（六）制定年度工作计划并报告其成果。

（七）回答数据主体的咨询和请求。

（八）与监管机构合作并作为其联系人。

第五十一（五十二）条 预防违法模型的认证许可、登记和监督。监管机构将负责认证预防违法模型符合法律和法规所规定的要求和要素，并对其进行监督。

监管机构将拥有有效认证的实体记入国家处罚与合规登记册。

由财政部发布并由总统府秘书长和经济、发展和旅游部长签署的条例将规定预防违法模型的实施、认证、登记和监督的要求、方式和程序。

第五十二（五十三）条 认证许可的有效期。由监管机构颁发的证书有效期为三年。在不影响上述规定的前提下，有下列情形之一的，认证许可将无效：

（一）由监管机构撤销。

（二）自然人数据控制者死亡。

（三）法人解散。

（四）司法判决执行。

（五）数据控制者自愿停止活动。

由于上述任何原因，只要证书不从登记册中删除，认证许可的有效期将无法对第三方强制执行。

第五十三（五十四）条 认证许可吊销。如果数据控制者不遵守本节的规定，监管机构可以吊销上述条款中指明的认证许可。为此，监管机构可要求提供履行其职能所需的所有信息。

当所要求的信息受到保密义务保护时，数据控制者可以不提供该信息，但必须证明该情况。

未能提供所需信息，以及提供虚假、不完整或明显错误的信息，将依照本法予以处罚。

当证书被机构吊销后，为了再次申请，数据控制者必须明确证明导致其吊销的原因已得到纠正。

第八章

国会、司法机构和享有宪法自治权的公共机构对个人数据的处理

第五十四（五十五）条 个人数据处理的一般规则。国会、司法部、共和国总审计署、检察院、宪法法院、中央银行、选举事务机关、司法选举机关和其他依法设立的特别法庭，根据各自组织法中的特别规定以及本法第四章适用于公共机构的规定，在其权力范围内履行法定职能，其对个人数据的处理是合法的，但本法第十四条之五和第四十四至四十六条关于共和国总审计署干预行政责任的认定以及第18834号法律适用的规定除外。这些机构的公务员必须对此类数据严格保密。在这些条件下，上述机构和组织拥有数据的控制权，且无需数据主体的同意就可以处理其个人数据。

这些机构内部机关的管理层必须发布必要的政策、法规和指示，以履行本法规定的原则和义务，尤其是那些允许行使数据主体权利的法规，以及个人数据处理时必须遵守的监管、安全和保护标准或最低条件，并可能为此需要监管机构的技术援助。同样，这些机构将对其官员在个人数据处理过程中发生的违规行为行使纪律处分权，特别是本法第三十四条之二、之三和之四所述的违规行为。

第五十五（五十六）条 行使权利和诉讼。数据主体可以在国会、司法部、共和国总审计署、检察院、宪法法院、中央银行、选举事务机关、司法选举机关和其他依法设立的特别法庭，以及由这些体制机构设立的机构前，根据上条规定以合理公平的程序行使本法规定的权利。

共和国总审计署、检察院、中央银行或选举事务机关无理或任意拒绝数据主体行使本法规定的权利，或违反本法第三条规定的任何原则、职责或义务，并且造成伤害的，或数据主体若因该机构的决定而感到不满或受到影响的，可根据本

法第四十三条规定的程序向上诉法院提起诉讼。

国会、司法部、宪法法院、司法选举机关和其他依法设立的特别法庭，必须确保这些机构对个人数据的处理严格遵守本法第三条中规定的原则和义务，确保本法规定的数据主体的权利得到尊重，并为此目的采取必要和适当的监察和内部控制措施。

过渡条款

第一条 本法第一、第二和第三条所列的对第19628号法律《个人数据保护法》和第20285号法律《公共信息获取法》以及2019年由经济、发展和旅游部颁布的第3号具有法律效力的法令《重新起草并加以协调与系统化第19496号法律〈制定保护消费者权益的规则〉》的修正，将在本法在《国家公报》上公布后第二十四个月的第一天分别生效。

第二条 本法所指条例必须在本法于《国家公报》上公布后的六个月内公布。

第三条 在本法第一条所列的对第19628号法律的修正生效前六十天内，民政局必须取消第19628号法律现行第二十二条规定的个人数据库登记。

第四条 个人数据保护监管局管理委员会委员、委员会主席和副主席的首次任命将在本法生效前六十天内进行。

在向参议院提出的首次任命提案中，需确定一名任期两年的委员、一名任期四年的委员和一名任期六年的委员。上述提案将作为单一法案提出，参议院必须作为一个整体对提案做出表决。

根据本法第一条过渡条款的规定，委员只有在本法生效后才能就职。

根据本法第三十条之八，该监管机构的章程必须在本法生效后九十天内向共和国总统提出。

第五条 设立预防负责人或个人数据保护专员的公共机构必须为此目的从各

自机构的现有工作人员中指定一名官员。

第六条 在本法生效的第一个预算年度，执行本法的最大财政支出将由经济、发展和旅游部预算内资源提供经费，经费不足部分，记入相应预算年度的公共财政预算项目。随后几年，将被纳入《公共部门预算法》。

对其他法律的修正

第二条 删除第20285号法律《公共信息获取法》第一章第三十三条第十三项。

第三条 将经济、发展和旅游部2019年第3号法令第十五条之二由以下内容替换，此法令确立了第19496号法律的合并、协调和系统化文本，第19496号法律确立了保护消费者权利的规则：

“第十五条之二 第二条之二第二项和第五十八条之二的规定在消费者关系框架内适用于消费者的个人数据”。

/Carey

第19628号法律：关于个人数据保护