GRIFOLS

Global Privacy and Data Protection Policy

SELECT YOUR LANGUAGE / ELIGE TU IDIOMA

GRIFOLS

Global Privacy and Data Protection Policy

CHINESE (SIMPLIFIED) / 简体中文

索引

GRIFOLS

1. 目的

本隐私和数据保护政策（“政策”）旨在解释所有 基立福 集团公司（“基立福”）为保护和保障个人数据而遵循的相关隐私原则，以及如何实施这些原则。

培养尊重个人数据的文化能够加强信任关系，并助力 基立福 实现改善全球民众健康与福祉的使命。

2. 范围

本政策适用于所有 基立福 集团公司，但不影响适用于其业务活动的任何数据保护法规或当地法律，与本政策之规定相比，这些法规或法律的隐私和数据保护规定可能更严格，也可能更宽松。因此，本政策的规定应结合适用法律进行解释和实施。

具体而言，本政策适用于在基立福 开展业务活动中处理个人数据的所有基立福 员工（“员工”）。个人数据是能直接用于或结合其他信息后用于识别个人身份的任何信息。

本政策不适用于非个人数据的信息或数据。

3. 相关文件

- 基立福 *行为准则*
- 基立福 *人权政策*
- *供应商全球条款和条件*
- *信息安全政策 - “Information Security Policy” (GHTI-CTRL-000237)*
- *信息技术使用政策 – “Information Technology Usage Policy” (CTRL-000110)*
- *个人数据事故程序 (DPO-SOP-000001)*
- *记录保留政策 – “Records Retention Policy” (ID448)*

您可以在内网的 Data Protection Office 部分找到更多有关 基立福隐私政策的信息。

4. 定义

在本政策中，下列术语应具有如下含义：

术语	定义
同意	对个人意愿的任何自愿、具体、知情和明确的表示，个人通过声明或明确的肯定举动，表明同意处理与其有关的个人数据。
控制者	决定个人数据处理的目的和手段的自然人或法人、公共机构、专门机构或其他团体。
„*Corporate Data Protection Office*“	负责在数据保护方面为基立福集团公司提供支持的企业部门。
数据保护/隐私法规	适用于基立福的任何法律、规则、法令、法案、决议、守则、准则或规定，包括与世界任何国家的个人数据的隐私或处理相关的修正案或替代条款，包括但不限于 GDPR。
数据保护专员 – *“Data Protection Officer “* (DPO)	负责告知、建议和监控基立福内部数据保护事项的正确合规情况的指定自然人或法人，同时担任基立福、数据主体和主管数据保护机构 (DPA) 之间的联系人。

术语	定义
数据主体/个人	基立福正在处理其个人数据并可根据可用的个人数据直接或间接将其识别的任何人（例如：员工、客户、捐赠者、患者等）。
《通用数据保护条例》(GDPR)	2016 年 4 月 27 日，欧洲议会和欧盟理事会通过了关于保护自然人处理个人数据和自由传输个人数据的 (EU) 2016/679 号条例，并废除第 95/46/EC 号指令。
个人数据/个人信息	与可识别或已被识别的个人有关的任何信息： 可通过该信息直接识别个人（例如：姓名、身份证号码、照片等） 可通过该信息与其他数据的结合间接识别个人（例如：健康记录、绩效评估、IP 地址等）。
个人数据泄露/事件	这种安全事件是指导致个人数据在由基立福或代表基立福的第三方传输、存储或以其他方式处理过程中，发生意外或非法的销毁、丢失、更改、泄露或被访问的情况。所有的个人数据泄露都属于安全事件，但并非所有安全事件都是个人数据泄露。
隐私声明	发送给个人的、包含与个人数据处理相关之信息的文件。
处理	涉及个人数据的任何自动或非自动操作（例如：收集、记录、存储、托管、修改、协商、使用、出版传播、擦除等。）
特殊类别的个人数据/敏感个人数据	法律认定为敏感的个人数据，因其私人性质应得到更高程度的保护，且只能在有限的情况下处理。具体示例如下： 种族或族裔血统 政治观点 宗教或哲学信仰 工会成员资格 遗传数据 专用于识别人类个体而被处理的生物特征数据 健康相关数据 有关性生活或性取向的数据 刑事定罪及罪行 受保护的健康信息 (*Protected Health Information,* PHI)
监管局/数据保护机构 (DPA)	负责监控和执行数据保护法律法规应用的独立公共机构。DPA 还就法律的解释提供指导，并视情况对不合规行为进行处罚。
第三方	指处理者以外的自然人或法人、公共机构、机关或组织，经授权可处理数据主体的个人数据，且与基立福有业务往来且不是基立福集团公司或员工。

5. 角色和责任

基立福 的隐私和数据保护从高层开始，由执行管理层领导。作为《基立福 行为准则》中的一项原则，它是我们企业文化和商业活动中不可分割的一部分，与公司内部的每一个人息息相关。

员工

在职业活动中需要处理个人数据的所有 基立福 员工均有义务遵守本政策。若员工对本政策的应用有任何疑问或要报告任何发现的潜在违规行为，则应联系其所属组织中负责隐私事务的人员或部门，或联系 *Corporate Data Protection Office* (privacy@grifols.com)。

Corporate Data Protection Office

Corporate Data Protection Office 负责制定 基立福 的全球隐私框架，并监督和协调数据保护法规的遵守情况。

它与 基立福 的所有部门和业务单位合作，提高全体员工在数据保护方面的意识，推动隐私文化建议，并提供可支持隐私合规运营的解决方案。其最终目标是实现对公众隐私权和个人数据保护的尊重。

数据保护专员 – Data Protection Officer (DPO)

对于已任命 DPO 的集团公司，其职责包括：

- 就适用数据保护法规进行告知、建议及合规监督，包括对数据处理相关人员的意识培养与培训。
- 提供数据保护影响评估建议并监督实施。
- 在所有涉及个人数据处理的事项上与监管机构合作。
- 作为监管机构和利益相关方的联络点。

DPO 在履行其职能时，应充分考虑到与数据处理操作相关的风险，同时考虑处理的性质、范围、背景和目的。

信息技术部门

IT 部门有责任确保根据本政策中的所有原则，实施与处理个人数据风险相称的技术和组织安全措施。

6. 政策

基立福从事的每项活动几乎都涉及处理来自广泛利益相关者的个人数据，这些利益相关者包括但不限于员工、患者、医疗专业人士、客户、投资者、供应商和捐助者。

基立福尊重任何将其个人数据委托给 基立福 并承诺遵守所有适用隐私法规的个人的隐私权。 .

基立福对透明度、诚信以及本文件中所述原则的承诺不仅限于符合法规要求。基立福通过提高员工对“什么是个人数据”及“如何保护个人数据”的认识，鼓励员工建立隐私和数据保护文化，并且在 基立福 ， 我们寻求从设计着手保护隐私以及默认保护隐私的方法。通过这种方法，基立福 与利益相关者建立了信任关系，降低了个人数据泄露的风险以及由此带来的声誉和经济损失，从而促进了 基立福 的长期可持续发展和对社会的承诺。

6.1.个人数据保护原则

所有处理个人数据的 基立福 员工均受本政策约束，并应遵守以下原则：

a. 以合法、公平及透明的方式处理个人数据。 员工应始终确保 基立福 具备适用的充分法律依据来处理个人数据。一般而言，数据保护法规中规定的法律依据包括但不限于为履行合同（例如雇佣合同）而处理个人数据，为遵守适用的法律义务（例如向税务机关传输个人数据）而处理个人数据，或出于 基立福 的合法利益而处理个人数据，前提是该等利益不优先于数据主体的权利和自由（例如防止欺诈）。如适用的数据保护法规所述，必须提前通知数据主体其个人数据将如何处理、谁将负责处理其数据以及向谁披露这些数据等事宜。

b. 仅为特定、明确及合法的目的收集个人数据。 仅允许员工为合法的特定明确目的收集个人数据，不得将个人数据用于向数据主体披露之外的其他目的。若需要变更处理目的，必须事先告知数据主体，并可能需要其他法律依据作为支持，同时需要征得数据主体的同意。

c. 仅处理与处理目的相符、相关且必要的个人数据（数据最小化原则）。 员工仅能处理为向数据主体披露之特定目的所需的最少量个人数据。如果不需全部或某些类型的个人数据，则既不得要求提供也不处理该等数据。

d. 仅处理准确并及时更新的个人数据。 员工应采取一切合理措施，确保在个人数据的整个信息生命周期内（即从收集到销毁）所处理的个人数据准确且及时更新。为此，员工应尽一切合理努力及时纠正或删除不准确的个人数据。如相关政策和程序所述，这可能需要基立福**内若干部**门的参与和合作。

e. 仅在为实现处理目的所必需的期限内且符合法律要求的期限内保留个人数据。 员工应仅在为满足处理个人数据之目的的需要或应法律要求的情况下，将个人数据保存在 基立福 **的文件中**（电子和纸质格式）。当个人数据不再需要保存时，员工应采取一切合理措施删除个人数据。如相关政策和程序所述，这可能需要基立福 **内若干部**门的参与和合作。

f. **以安全的方式**处理个人数据。 基立福 应采取组织性和技术性的安全措施，以保护个人数据，确保其机密性和可用性，并在适用情况下，依据相关法规以安全的方式进行共享。所有 基立福 **的**员工都必须遵守适用的技术和组织安全措施，尤其在处理特殊类别的个人数据时，这些措施尤为重要。

6.2.**数据主体**对其个人数据的权利

数据保护法规赋予个人若干权利，包括访问其个人数据、要求纠正任何错误的个人数据或要求删除其个人数据等。在基立福 **向个人提供的**隐私声明中，明确规定了这些权利的具体内容以及如何行使这些权利。

根据适用法律法规，个人对其个人数据享有的权利可能包括以下内容：

- 信息权：有权获得有关个人数据处理的简明、透明、易懂和易于访问的信息。一般而言，基立福在隐私声明中提供的信息包括控制者和数据保护专员的联系方式、处理数据的目的和法律依据（原因）、接收者的类别（若有）、个人数据的保存期限以及下文提及的数据保护权利等。DPO 和基立福 的法律顾问将与员工合作，根据需要编制和/或修改隐私声明。
- 访问权：有权要求确认是否正在处理个人数据，如果正在处理，有权获得查阅 基立福文件中的个人数据的权利。
- 修正权：有权要求修改不准确的个人数据。
- 删除权：有权要求删除个人数据。
- 反对权：有权要求在特定情况下不处理个人数据。
- 可转移权：有权要求在电子文件中接收提供给 基立福 的个人数据，并有权将其传输给其他当事方
- 限制处理权：在以下情况中，有权要求限制对个人数据的处理：
  i. **在个人数据受到**质疑后，正在核实其准确性；
  ii. 处理个人数据属违法行为，并且数据主体反对删除；
  iii. **出于数据**处理之目的，基立福 **不再需要某些个人数据，但个人需要**这些数据来确立、行使或抗辩法定求偿权，和
  iv. **数据主体**对基于公共利益或合法权益的数据处理提出反对，就执行任务而处理数据，同时正在核实 基立福 **的合法理由是否**优先于数据主体的合法理由。
- 撤回同意权：有权撤回所提供的同意，但不影响基于撤回同意前提供的同意进行处理的合法性。

基立福 **建立了内部程序，以促**进和管理个人行使数据保护权。任何 基立福 **的**员工在收到数据主体的权利请求时，应立即联系其所在组织中负责数据保护的人员或部门；如无相关负责人，则应联系企业 *Corporate Data Protection Office* (privacy@grifols.com)

6.3.个人数据保留

当出于处理个人数据的目的或履行适用的法律义务而不再需要个人数据时，员工应采取一切合理措施销毁或删除个人数据的所有副本，无论以纸质介质或任何其他物理或数字介质存储。

有关此主题的更多信息，请参阅 基立福 **数据保留政策** (*"Records Retention Policy"* ID448)。

6.4.个人数据安全和数据泄露

基立福 制定了适当的程序和技术措施，以确保个人数据在整个保存期间的安全，采取合理的技术和组织措施来确保个人数据的安全，并重点关注特殊类别的个人数据。基立福还建立了定期测试、评估和评定这些措施有效性的流程，以确保：

a. 个人数据的可用性：业务信息系统和个人数据能够按要求的方式和时间使用。基立福 采取合理措施，在发生物理或技术事件时及时恢复个人数据，以防止意外或未经授权的损失、破坏或损坏。

b. 个人数据的机密性：存储个人数据的系统和文件仅可由经过授权的人员访问，防止未经授权、意外或非法访问或披露个人数据。

c. 个人数据的完整性：保持个人数据的准确性，以防止意外或欺诈性更改。

所有员工在处理个人数据时应遵守适用的基立福 信息安全政策和程序，包括但不限于 IT 安全政策。

个人数据泄露是危害个人数据可用性、机密性或完整性的安全事故。基立福 制定了程序 (DPO-SOP-000001_Personal Data Incident Procedure)，供员工报告安全事件和个人数据泄露，以使 基立福 能够进行相应的风险和安全评估，并在适用的情况下，履行其通知数据保护机构和受影响数据主体的义务。

6.5.个人数据传输和服务提供商

在正常业务过程中，员工可能出于合法业务原因或在法律另外允许或要求时，需要与 基立福 的集团公司或多个国家的第三方签订服务合同和/或将个人数据传输给 基立福 的集团公司或第三方。

因雇佣第三方提供新服务（无论是现有供应商还是新供应商）且涉及处理个人数据时，必须进行供应商评估，以评估该等处理对数据主体权利和自由的风险和影响。评估的目的是确认供应商能够按照本政策和适用数据保护法规规定的原则和标准保护和处理个人数据。

与参与个人数据处理的第三方或 基立福 集团公司签订的所有服务协议必须包含数据保护条款或对已签署的数据保护协议的引用。

个人数据跨境传输只有在具备适当保障措施的情况下才能获得批准。

基立福 建立了内部程序，以验证个人数据跨境传输和服务提供商的合同符合适用的数据保护法规。

6.6.培训和认识

基立福 试图在公司内建立强大的隐私保护文化。基立福 根据员工处理个人数据的实际情况，推行并提供相称的适当培训，旨在帮助员工提高认识，并教育他们如何以符合 基立福 标准和程序以及适用的数据保护法规的方式识别和处理个人数据。

6.7.从设计着手保护隐私与默认保护隐私

员工应在个人数据的整个生命周期（即从收集到销毁）内考虑隐私和数据保护问题，因此应将数据保护原则和安全措施纳入其在 基立福 的业务活动中，尤其在实施新项目时。此外，还应采取适当的技术和组织安全措施，以确保只处理严格必需的个人数据。

7. 变更原因

更新定义和相关文件。

GRIFOLS

Global Privacy and Data Protection Policy

CZECH / ČESKY

INDEX

1. ÚČEL

Účelem této politiky ochrany soukromí a osobních údajů („politika“) je vysvětlit příslušné zásady ochrany osobních údajů, které se vztahují na společnosti skupiny Grifols Group (dále jen "Grifols") pro ochranu a zabezpečení osobních údajů a jak jsou tyto zásady implementovány.

Podpora kultury respektu k osobním údajům posiluje vztahy důvěry a přispívá k poslání společnosti Grifols zlepšovat zdraví a pohodu lidí na celém světě.

2. ROZSAH PLATNOSTI

Tato politika platí pro všechny společnosti ze skupiny Grifols bez dotčení jakýchkoli předpisů nebo místních zákonů o ochraně osobních údajů platných pro obchodní činnosti společnosti Grifols, jejichž ustanovení o ochraně soukromí a osobních údajů mohou být méně přísná nebo naopak přísnější než ustanovení uvedená v této politice. Ustanovení této politiky musí být vykládána a uplatňována v souladu s platnými právními předpisy.

Tato politika platí zejména pro všechny zaměstnance společnosti Grifols („zaměstnanci“), kteří zpracovávají osobní údaje v rámci obchodních činností vykonávaných společností Grifols. Osobní údaje jsou veškeré informace, které umožňují přímo nebo společně s dalšími informacemi zjistit totožnost jednotlivých osob.

Tato politika se nevztahuje na informace či údaje, které nejsou osobními údaji.

3. SOUVISEJÍCÍ DOKUMENTY

- *Etický kodex společnosti Grifols*
- *Politika společnosti Grifols v oblasti lidských práv*
- *Globální obchodní podmínky pro dodavatele*
- *Politika bezpečnosti informací” (“Information Security Policy” / GHTI-CTRL-000237)*
- *Politika používání informačních technologií” (“Information Technology Usage Policy” CTRL-000110)*
- *Postup při incidentu s osobními údaji (DPO-SOP-000001)*
- *Politika archivace záznamů (“Records Retention Policy” ID448)*

Další informace o ochraně osobních údajů ve společnosti Grifols naleznete na intranetu v sekci "Data Protection Office".

4. DEFINICE

Pro účely této politiky mají níže uvedené pojmy následující význam:

POJEM	DEFINICE
Souhlas	Svobodně udělené, konkrétní, informované a jednoznačné vyjádření přání jedince, který ve svém prohlášení nebo jasným stvrzujícím úkonem projeví souhlas se zpracováním osobních údajů vztahujících se k jeho osobě.
Správce	Fyzická nebo právnická osoba, veřejný úřad, agentura či jiný orgán, který stanoví účel a význam zpracování osobních údajů.
„*Corporate Data Protection Office*“	Korporátní oddělení pro ochranu osobních údajů pověřené podporou společností skupiny Grifols v záležitostech ochrany osobních údajů.

POJEM	DEFINICE
Předpisy týkající se ochrany osobních údajů	Jakýkoli zákon, nařízení, stanovy, předpis, usnesení, kodex, průvodce nebo ustanovení, včetně změn nebo náhrad, týkající se ochrany osobních údajů nebo zpracování osobních údajů jednotlivců v jakékoli zemi na světě, kterým společnost Grifols podléhá, mimo jiné včetně GDPR.
Pověřenec pro ochranu osobních údajů (DPO)	Osoba, jejímž úkolem je informovat, radit a sledovat správné dodržování předpisů v oblasti ochrany osobních údajů ve společnosti Grifols, a která také slouží jako kontaktní osoba mezi společností Grifols, subjekty údajů a úřadem pro ochranu osobních údajů (DPA).
Subjekt údajů / osoba	Jakákoli osoba, jejíž osobní údaje zpracovává společnost Grifols a kterou lze přímo či nepřímo identifikovat na základě těchto dostupných osobních údajů (např. zaměstnanci, klienti, dárci, pacienti atd.).
Obecné nařízení o ochraně osobních údajů (GDPR)	Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES.
Osobní údaje / osobní informace	Veškeré informace týkající se osoby, která může být identifikovaná nebo identifikovatelná: - přímo uvedením dané informace (např. jméno, identifikační číslo, fotografie atd.) - nepřímo z dané informace v kombinaci s dalšími údaji (např. zdravotní záznamy, hodnocení výkonu, IP adresa atd.).
Incident/porušení osobních údajů	Jakýkoli bezpečnostní incident, který má za následek náhodné nebo nezákonné zničení, ztrátu, změnu, sdělení nebo přístup k osobním údajům přenášeným, uloženým nebo jinak zpracovávaným společností Grifols nebo třetí stranou jménem společnosti Grifols. Všechna porušení zabezpečení osobních údajů jsou incidenty, ale ne všechny incidenty jsou nutně porušením zabezpečení osobních údajů.
Oznámení o ochraně osobních údajů	Dokument adresovaný jednotlivým osobám, který obsahuje informace o zpracování osobních údajů.
Zpracování	Automatizovaná nebo neautomatizovaná operace, která zahrnuje osobní údaje (např. sběr dat, zaznamenávání, uložení, hosting, úprava, prohlížení, poradenství, použití, přenos publikací, výmaz atd.).
Zvláštní kategorie osobních údajů / citlivé osobní údaje	Jedná se o osobní údaje, které zákon považuje za citlivé a vyžadující tudíž vyšší stupeň ochrany z důvodu jejich soukromé povahy a které lze zpracovávat pouze za určitých omezených okolností. Níže je uvedeno několik příkladů: - Rasový nebo etnický původ - Politické názory - Náboženské vyznání či filozofické přesvědčení - Členství v odborech - Genetické údaje - Biometrické údaje sloužící výhradně k identifikaci fyzické osoby - Údaje o zdravotním stavu - Údaje o sexuálním životě nebo sexuální orientaci - Odsouzení a trestné činy - Chráněné zdravotní informace (*Protected Health Information,* PHI)

POJEM	DEFINICE
Dozorový úřad / úřad pro ochranu osobních údajů (DPA)	Nezávislý veřejný orgán odpovědný za dohled a prosazování zákonů a předpisů o ochraně osobních údajů. Úřad pro ochranu osobních údajů také poskytuje pokyny k výkladu právních předpisů a případně ukládá sankce za jejich nedodržení.
Třetí strana	Třetí strany fyzické nebo právnické osoby, orgány veřejné moci, služby nebo subjekty jiné než správce údajů, které jsou oprávněny zpracovávat osobní údaje subjektů údajů, se kterými společnost Grifols komunikuje a které nejsou společností nebo zaměstnancem společnosti Grifols.

5. ÚLOHY A ODPOVĚDNOSTI

Ochrana soukromí a osobních údajů ve společnosti Grifols začíná na nejvyšší úrovni, řízena výkonným vedením. Je jakožto jedna ze zásad etického kodexu společnosti Grifols nedílnou součástí naší kultury a obchodních činností a týká se každého ve společnosti.

Zaměstnanci

Všichni zaměstnanci společnosti Grifols, kteří zpracovávají osobní údaje v rámci své profesní činnosti, jsou povinni dodržovat tyto zásady. Zaměstnanci by se měli obrátit na osobu nebo oddělení odpovědné za ochranu údajů ve své organizaci nebo, pokud to není možné, na *Corporate Data Protection Office* (privacy@grifols.com), pokud mají jakékoli dotazy týkající se jejich uplatňování, a také nahlásit jakékoli potenciální porušení tohoto pravidla.

Corporate Data Protection Office

Corporate Data Protection Office údajů je zodpovědné za definování globálního rámce ochrany osobních údajů společnosti Grifols a za dohled a koordinaci dodržování předpisů o ochraně osobních údajů.

Spolupracuje se všemi odděleními a obchodními jednotkami společnosti Grifols na posílení úrovně znalostí o ochraně údajů mezi všemi zaměstnanci, podporuje kulturu ochrany osobních údajů a poskytuje řešení, která umožňují provozní soulad s předpisy o ochraně údajů. Konečným cílem je dosáhnout respektování práva lidí na soukromí a ochranu jejich osobních údajů.

Pověřenec pro ochranu osobních údajů (DPO)

Ve společnostech skupiny, ve kterých byl pověřenec pro ochranu osobních údajů jmenován, bude odpovědný za následující funkce:

- Informovat, radit a sledovat dodržování platných předpisů o ochraně údajů, včetně informovanosti a školení pracovníků zapojených do operací zpracování údajů.
- Poskytovat poradenství při posuzování vlivu na ochranu osobních údajů a sledovat jejich provádění.
- Spolupracovat s dozorovým úřadem ve všech záležitostech týkajících se zpracování osobních údajů.
- Působí jako kontaktní místo pro orgán a zúčastněné strany

Pověřenec pro ochranu osobních údajů vykonává své funkce s náležitým ohledem na rizika spojená s operacemi zpracování, s přihlédnutím k povaze, rozsahu, kontextu a účelům zpracování.

Oddělení informačních technologií (IT)

Oddělení IT je odpovědné za zajištění toho, aby byla zavedena technická a organizační bezpečnostní opatření přiměřená riziku spojenému se zpracováním osobních údajů, a to v souladu se všemi zásadami stanovenými v těchto zásadách.

6. POLITIKA

Většina činností prováděných společností Grifols zahrnuje zpracování osobních údajů různých zúčastněných stran, včetně zaměstnanců, pacientů, zdravotnických pracovníků, zákazníků, investorů, dodavatelů a dárců.

Společnost Grifols respektuje právo na ochranu osobních údajů osob, které jí svěřují své osobní údaje, zavazuje se dodržovat platné předpisy o ochraně osobních údajů.

Závazek společnosti Grifols k transparentnosti, integritě a zásadám popsaným níže přesahuje pouhé dodržování předpisů. Společnost Grifols podporuje kulturu ochrany soukromí a osobních údajů tím, že zvyšuje povědomí zaměstnanců o tom, co jsou zač a jak je chránit, a také tím, že zaujímá přístup založený na ochraně soukromí již od návrhu a ve výchozím nastavení.

Tímto způsobem společnost Grifols vytváří vztahy důvěry se svými partnery a zmírňuje riziko narušení bezpečnosti osobních údajů s následným ekonomickým poškozením a poškozením pověsti, čímž přispívá k dlouhodobě udržitelnému růstu a závazku společnosti Grifols vůči společnosti.

6.1. Zásady ochrany osobních údajů

Všichni zaměstnanci společnosti Grifols, kteří zpracovávají osobní údaje, podléhají těmto zásadám a musí dodržovat následující zásady:

a. Zpracování osobních údajů zákonným, poctivým a transparentním způsobem. Zaměstnanci musí vždy zajistit, aby společnost Grifols měla odpovídající právní důvody pro zpracování osobních údajů fyzických osob. Obecně platí, že právní základy jsou stanoveny v předpisech o ochraně osobních údajů a zahrnují mimo jiné zpracování osobních údajů za účelem plnění smlouvy (např. pracovní smlouvy), splnění platné právní povinnosti (např. hlášení osobních údajů daňové správě) nebo oprávněné zájmy společnosti Grifols, pokud nepřevažují nad právy a svobodami subjektů údajů (např. prevence podvodů). V souladu s ustanoveními platných předpisů o ochraně osobních údajů musí být subjekty údajů mimo jiné předem informovány o tom, jak budou jejich osobní údaje zpracovávány, kdo bude odpovědný za zpracování jejich údajů a komu mohou být sděleny.

b. Sběr osobních údajů pouze pro konkrétní, jednoznačné a legitimní účely. Zaměstnanci mají povoleno shromažďovat osobní údaje pouze pro konkrétní a jednoznačný účel (případně účely), který je / které jsou zákonné, a nemohou osobní údaje používat k jiným účelům než k těm, které oznámily subjektům údajů. Změny účelu zpracování musí být subjektu údajů sděleny předem, může být nutné je podložit odlišným právním odůvodněním a může být zapotřebí si od subjektu údajů vyžádat souhlas.

c. Zpracování pouze těch osobních údajů, které jsou přiměřené, relevantní a omezené na to, co je nezbytné z hlediska účelů zpracování (minimalizace údajů). Zaměstnanci budou zpracovávat pouze minimum osobních údajů potřebných pro konkrétní účel, který byl subjektu údajů sdělen. Pokud takové údaje nejsou vyžadovány, nesmí být žádným způsobem požadovány ani zpracovávány.

d. Zpracovávání pouze osobních údajů, které jsou přesné a aktuální. Zaměstnanci musí podniknout veškeré přiměřené kroky, aby zajistili, že osobní údaje, které zpracovávají, jsou přesné a aktuální v průběhu celého životního cyklu informací (tj. od shromažďování až po likvidaci). V tomto ohledu zaměstnanci vynaloží veškeré přiměřené úsilí, aby neprodleně opravili nebo vymazali nepřesné osobní údaje, což může vyžadovat zapojení a spolupráci různých oddělení společnosti Grifols, jak je popsáno v příslušných zásadách a postupech.

e. Uchovávání osobních údajů po dobu ne delší, než je nezbytné pro účely, pro které jsou zpracovávány. Zaměstnanci budou uchovávat osobní údaje v souborech společnosti Grifols (v elektronické i papírové podobě) pouze po dobu nezbytně nutnou k naplnění účelů, pro které jsou osobní údaje zpracovávány, nebo pokud je to nezbytné ze zákona. Zaměstnanci podniknou veškeré přiměřené kroky k vymazání osobních údajů, pokud již nejsou potřebné, což může

vyžadovat zapojení a spolupráci různých oddělení společnosti Grifols, jak je popsáno v příslušných zásadách a postupech.

f. Zpracovávání osobních údajů bezpečným způsobem Společnost Grifols přijme technická a organizační bezpečnostní opatření k ochraně osobních údajů, zajištění jejich důvěrnosti, integrity a dostupnosti a případně je bude sdílet bezpečně a v souladu s předpisy. Všichni zaměstnanci společnosti Grifols musí dodržovat platná technická a organizační bezpečnostní opatření, která jsou zvláště důležitá při zpracování zvláštních kategorií osobních údajů.

6.2. Práva fyzických osob k jejich osobním údajům

Předpisy o ochraně osobních údajů udělují osobám několik práv, mimo jiné včetně získání přístupu ke svým osobním údajům, právo na opravu chybných osobních údajů nebo právo na vymazání osobních údajů. Tato práva a možnost, jak je uplatnit, jsou jasně stanovena v oznámeních o ochraně osobních údajů společností Grifols, která společnost dává osobám k dispozici.

V závislosti na platných předpisech mohou práva subjektů údajů ve vztahu k jejich osobním údajům zahrnovat následující:

- Informace: právo obdržet stručné, transparentní, srozumitelné a snadno přístupné informace o zpracování osobních údajů. Společnost Grifols obecně tyto informace poskytne mimo jiné v oznámení o ochraně osobních údajů, které mimo jiné obsahuje kontaktní údaje správce údajů a pověřence pro ochranu osobních údajů, účely a právní základ (proč) zpracování, kategorie příjemců (pokud existují), dobu uchování osobních údajů a práva na ochranu osobních údajů uvedených dále. DPO a právní poradci společnosti Grifols ve spolupráci se zaměstnanci podle potřeby vypracují anebo zrevidují oznámení o ochraně osobních údajů.
- Přístup: právo požadovat potvrzení, zda byly či nebyly zpracovány osobní údaje, a pokud ano, právo získat přístup k osobním údajům uloženým ve složkách společnosti Grifols.
- Oprava: právo požadovat úpravu nepřesných osobních údajů.
- Výmaz: právo požadovat vymazání osobních údajů.
- Námitka: Právo požadovat, aby osobní údaje nebyly za konkrétních okolností zpracovány.
- Přenositelnost: právo požadovat přijetí osobních údajů poskytnutých společnosti Grifols v elektronickém souboru, stejně jako právo na přenos takových údajů dalším stranám.
- Omezení zpracování: právo požadovat omezení zpracování osobních údajů v kterémkoli z těchto případů:
  i. pokud se ověřuje přesnost osobních údajů, jestliže byla popřena jejich přesnost;
  ii. pokud je zpracování osobních údajů protiprávní a subjekt údajů odmítá výmaz osobních údajů;
  iii. společnost Grifols již osobní údaje nepotřebuje pro účely zpracování, ale subjekt údajů je požaduje pro určení, výkon nebo obhajobu právních nároků;
  iv. subjekt údajů vznesl námitku proti zpracování na základě oprávněného zájmu nebo veřejného zájmu, a to na dobu nezbytnou k ověření, zda oprávněné důvody společnosti Grifols převažují nad důvody subjektu údajů.
- Odvolání souhlasu: právo odvolat udělený souhlas, aniž by byla dotčena zákonnost zpracování vycházejícího ze souhlasu, který byl dán před jeho odvoláním.

Společnost Grifols zavádí interní postupy pro usnadnění a správu výkonu práv fyzických osob na ochranu osobních údajů. Každý zaměstnanec společnosti Grifols, který obdrží žádost od subjektu údajů o uplatnění svých práv, musí neprodleně kontaktovat osobu nebo oddělení odpovědné za ochranu údajů ve své organizaci, nebo pokud takové nejsou, *Corporate Data Protection Office* společnosti (privacy@grifols.com).

6.3. Uchování osobních údajů

Pokud již nejsou osobní údaje nadále zapotřebí pro účel, pro něž byly zpracovány, nebo z důvodu splnění platných zákonných povinností, podniknou zaměstnanci všechny přiměřené kroky k likvidaci nebo

výmazu všech kopií těchto osobních údajů, ať už na papíře nebo na jakémkoli jiném fyzickém nebo elektronickém paměťovém médiu.

Další informace o tomto tématu jsou uvedeny v Politice uchovávání údajů společnosti Grifols (*"Records Retention Policy"* ID448).

6.4. Bezpečnost osobních údajů a narušení bezpečnosti

Společnost Grifols používá postupy a technologie k ochraně osobních údajů po dobu, po kterou je uchovává, a to přijetím přiměřených technických a organizačních opatření k zachování bezpečnosti osobních údajů, se zvláštním důrazem na zvláštní kategorie osobních údajů. Společnost Grifols také zavádí pravidelný proces kontroly, hodnocení a hodnocení účinnosti těchto opatření, aby zajistila, že:

a. Dostupnost osobních údajů: aby informační systémy a osobní údaje společnosti byly dostupné požadovaným způsobem a v požadovaném čase. Společnost Grifols přijímá přiměřená opatření k ochraně osobních údajů před náhodnou nebo neoprávněnou ztrátou, zničením nebo poškozením a k tomu, aby byla schopna rychle obnovit osobní údaje v případě fyzického nebo technického incidentu.

b. Zachování mlčenlivosti o osobních údajích: aby k systémům a souborům, které uchovávají osobní údaje, měly přístup pouze řádně oprávněné osoby, aby se zabránilo neoprávněnému, náhodnému nebo nezákonnému přístupu nebo sdělování osobních údajů.

c. Celistvost osobních údajů: k udržení přesnosti osobních údajů před náhodnou či podvodnou změnou.

Všichni zaměstnanci jsou při zpracování osobních údajů povinni dodržovat platné zásady a postupy společnosti Grifols v oblasti informační bezpečnosti, mimo jiné včetně „~~Politika~~ Politiky–bezpečnosti informací" .

Porušení zabezpečení osobních údajů je druh bezpečnostního incidentu, který ohrožuje dostupnost, důvěrnost nebo integritu osobních údajů. Společnost Grifols navrhla postupy (DPO-SOP-000001_ Postup pro incidenty týkající se osobních údajů), které umožňují zaměstnancům interně hlásit incidenty a narušení bezpečnosti osobních údajů, aby byla společnost Grifols schopna provést odpovídající posouzení rizik a bezpečnosti a případně splnit oznamovací povinnost úřadu pro ochranu osobních údajů a dotčených subjektů údajů.

6.5. Přenosy osobních údajů a poskytovatelé služeb

Při běžné obchodní činnosti se může stát, že zaměstnanci budou potřebovat uzavřít smlouvu o poskytování služeb anebo přenést osobní údaje do jiných společností skupiny Grifols nebo třetím stranám v některých zemích, a to z legitimních obchodních důvodů nebo pokud to jinak povoluje či vyžaduje zákon.

V případě, že je s třetí stranou (ať už se stávajícím nebo novým poskytovatelem) uzavřena smlouva o nové službě, jejíž součástí je zpracování osobních údajů, musí být provedeno posouzení poskytovatele, aby bylo posouzeno riziko a dopad takového zpracování na práva a svobody subjektů údajů. Účelem takového posouzení je potvrdit, že poskytovatel je schopen chránit a zpracovávat osobní údaje v souladu se zásadami a standardy stanovenými v těchto zásadách a v ustanoveních platných předpisů o ochraně osobních údajů.

Všechny smlouvy o poskytování služeb s třetími stranami nebo se společnostmi skupiny Grifols, které zahrnují zpracování osobních údajů, musí obsahovat doložky o ochraně údajů nebo odkaz na již formalizovanou smlouvu o ochraně údajů.

Přeshraniční předávání osobních údajů bude přijatelné pouze tehdy, budou-li zavedeny přiměřené záruky.

Společnost Grifols zavádí interní postupy pro ověřování, zda jsou přenosy osobních údajů mezi zeměmi a smluvní strany s poskytovateli služeb v souladu s platnými předpisy o ochraně osobních údajů.

6.6. Školení a povědomí

Společnost Grifols usiluje o podporu silné kultury ochrany osobních údajů ve společnosti. Za tímto účelem podporuje a poskytuje svým zaměstnancům odpovídající školení, které je úměrné zpracování osobních údajů, které provádějí, a jehož cílem je zvýšit povědomí a vzdělávat o tom, jak identifikovat a zpracovávat osobní údaje způsobem, který je v souladu s pravidly a postupy společnosti Grifols a platnými předpisy o ochraně údajů.

6.7. Záměrná a standardní ochrana osobních údajů

Zaměstnanci musí brát v úvahu otázky ochrany soukromí a údajů v průběhu celého životního cyklu osobních údajů (tj. od shromažďování až po likvidaci), a proto musí začlenit zásady ochrany osobních údajů a bezpečnostní opatření do všech profesních činností, které ve společnosti Grifols vykonávají. zejména při realizaci nového projektu. Kromě toho budou zavedena vhodná technická a organizační bezpečnostní opatření, aby bylo zajištěno, že budou standardně zpracovávány pouze osobní údaje nezbytně nutné pro každý účel.

7. DŮVODY ZMĚNY

Aktualizace definic a souvisejících dokumentů.

GRIFOLS

Global Privacy and Data Protection Policy

ENGLISH

INDEX

1. PURPOSE

The purpose of this Privacy and Data Protection Policy (the "policy") is to explain the relevant privacy principles applicable to all Group Grifols companies („Grifols“) for the protection and security of personal data and how these principles are implemented.

Fostering a culture of respect for personal data strengthens relationships of trust and contributes to Grifols' mission to improve the health and well-being of people around the world.

2. SCOPE

This policy applies to all Grifols' Group companies without prejudice to any data protection regulations or local laws applicable to its business activities, which may establish more or less stringent privacy and data protection provisions than the ones regulated in this policy. Therefore, the provisions of this policy should be interpreted and implemented in conjunction with applicable laws.

Specifically, this policy applies to all Grifols’ employees (the “employees”) who process personal data as part of the business activities carried out by Grifols. Personal data is any information that either directly or in combination with other information enables the identification of an individual.

This policy does not apply to information or data that is not personal data.

3. RELATED DOCUMENTS

- *Grifols' Code of Conduct*
- *Grifols' Human Rights Policy*
- *Vendors’ Global Terms and Conditions*
- *Information Security Policy (GHTI-CTRL-000237)*
- *Information Technology Usage Policy (CTRL-000110)*
- *Personal Data Incident Procedure (DPO-SOP-000001)*
- *Records Retention Policy (ID448)*

You can find more information about privacy in Grifols in the Data Protection Office section of the intranet.

4. DEFINITIONS

For the purpose of this policy, the terms indicated below shall have the following meaning:

TERM	DEFINITION
Consent	Any freely given, specific, informed and unambiguous indication of an individual’s wishes by which he or she, by a statement, or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.
Controller	Natural or legal person, public authority, agency or other body, which determines the purposes and means of the processing of personal data.
Corporate Data Protection Office	Corporate department tasked with supporting the Grifols group companies in data protection matters.
Data Protection/Privacy Regulations	Any law, rule, statute, act, resolution, code, guideline or provision, including its amendments or replacements related to privacy or the processing of personal data of individuals in any country of the world, applicable to Grifols, including without limitation GDPR.

TERM	DEFINITION
Data Protection Officer (DPO)	Natural or legal person designated with informing, advising and monitoring the correct compliance of data protection matters within Grifols and who also serves as a contact point between Grifols, the data subjects and the competent Data Protection Authority (DPA).
Data Subject / Individual	Any person whose personal data is being processed by Grifols and who can be identified, directly or indirectly on the basis of that available personal data (e.g. employees, clients, donors, patients, etc.).
General Data Protection Regulation (GDPR)	Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.
Personal Data / Personal Information	Any information relating to an individual who can be identified or who is identifiable: - Directly by reference to that information (e.g. name, ID number, photo, etc.) - Indirectly from that information in combination with other data (e.g. health records, a performance evaluation, IP address, etc.).
Personal Data Breach/Incident	A security incident that leads to the accidental or unlawful destruction, loss, alteration, communication of, or access to, personal data transmitted, stored or otherwise processed by Grifols or by a third party on behalf of Grifols. All personal data breaches are incidents, but not all incidents are necessarily Personal Data Breaches.
Privacy Notice	Document addressed to individuals that contains information on the processing of personal data.
Processing	Any automated or non-automated operation that involves personal data (e.g. collection, recording, storage, hosting, modification, consultation, use, publication transmission, erasure, etc.).
Special Categories of Personal Data / Sensitive Personal Data	Personal data considered by law to be sensitive and, therefore, deserving a higher degree of protection because of its private nature and which can only be processed in limited circumstances. The following are some examples: - Racial or ethnic origins - Political opinions - Religious or philosophical beliefs - Trade-union membership - Genetic data - Biometric data processed solely to identify a human being - Health-related data - Data concerning sex life or sexual orientation - Criminal convictions and offences - Protected Health Information (PHI)
Supervisory Authority / Data Protection Authority (DPA)	Independent public authority responsible for the monitoring and enforcement of the application of data protection laws and regulations. The DPA also provides guidance on the interpretation of the legislation and, as the case may be, imposes penalties for non-compliance.
Third Party	A natural or legal person, public authority, agency or body other than the processor, who is authorised to process data subjects' personal data, with whom Grifols interacts and that is not a Grifols' Group company or an employee.

5. ROLES AND RESPONSIBILITIES

Privacy and data protection at Grifols starts at the top, led by the Executive Management. As one of the principles in the Grifols' Code of Conduct, it is an integral part of our culture and business activities and concerns everyone within the company.

Employees

It is the obligation of all Grifols' employees who handle personal data as part of their professional activity to follow this policy. Employees should contact the person or department incharge of privacy in their organización or with the Corporate Data Protection Office (privacy@grifols.com) with any queries regarding the application of this policy and to report any identified potential violation.

Corporate Data Protection Office

The Corporate Data Protection Office is responsible for defining Grifols' global privacy framework and to oversee and coordinate compliance with data protection regulations.

It collaborates with all Grifols' departments and business units to strenghen the level of awareness on data protection matters among all employees fostering a privacy culture and providing solutions that allow for operational compliance with privacy regulations. Its ultimate goal is to achieve respect for prople's right to privacy and personal data protection.

Data Protection Officer (DPO)

For group companies in which a DPO has been appointed, he or she will be responsible for the following functions:

- Inform, advise and monitor compliance with applicable data protection regulations, including awareness and training of personnel involved in data processing operations.
- Provide advice on data protection impact assessments and monitor their implementation.
- Cooperate with the supervisory authority in all matters relating to the processing of personal data.
- Acting as a point of contact for the authority and stakeholders

The DPO shall carry out its functions with due regard to the risks associated with the processing operations, taking into account the nature, scope, context and purposes of the processing.

Information Technology Department

The IT department is responsible for ensuring that technical and organisational security measures proportional to the risk of the processing personal data are implemented according to all the principles included in this policy.

6. POLICY

Almost every activity that Grifols undertakes involves the processing of personal data from a wide range of stakeholders, including without limitation employees, patients, healthcare professionals, customers, investors, vendors and donors.

Grifols respects the privacy rights of any individuals who entrust Grifols with their personal data and is committed to comply with all applicable privacy regulations. .

Grifols' commitment to transparency, integrity and the principles detailed in this document extends beyond regulatory compliance. Grifols encourages a culture of privacy and data protection by raising employee awareness about what is and how to protect personal data and pursue an approach of privacy by design and privacy by default at Grifols. With this approach Grifols builds relationships of trust with its stakeholders and mitigates the risk of personal data breaches as well as the consequent reputational and economical damages , thus contributing to Grifols' long-term sustainable growth and its commitment to society.

6.1. Personal Data Protection Principles

All Grifols' employees processing personal data are bound by this policy and should abide by the following principles:

a. Process personal data lawfully, fairly and in a transparent manner. Employees should always ensure that Grifols has an adequate legal justification applicable to process personal data of individuals. In general, legal bases are set out in data protection regulations and these include without limitation, processing personal data to perform a contract (e.g. an employment contract), to comply with applicable legal obligations (e.g. to communicate personal data to tax authorities) or due to the legitimate interests of Grifols, provided that these do not override the rights and freedoms of the data subjects (e.g. fraud prevention). As set forth in the applicable data protection regulations, data subjects must be informed in advance about how their personal data will be processed, who will be responsible for the processing of their data and to whom it may be disclosed, among other aspects.

b. Collect personal data only for specified, explicit and legitimate purposes. Employees are permitted to collect personal data only for specific and explicit purpose(s) that is/are lawful and cannot use personal data for purposes other than for the purposes disclosed to the data subjects. Changes to the purpose of the processing have to be communicated to the data subject in advance and may need to be supported by a different legal basis and consent may need to be obtained from the data subject.

c. Process only personal data that is adequate, relevant and limited to what is necessary in relation to the purposes (data minimization). Employees shall only process the minimum personal data required for the specific purpose disclosed to the data subject. If personal data or certain types of personal data are not needed, they should neither be requested nor processed.

d. Process only personal data that is accurate and updated. Employees shall take all reasonable steps to process personal data that are accurate and updated throughout the information lifecycle (i.e., from collection to destruction). In this regard, employees shall make all reasonable efforts to rectify or erase inaccurate personal data promptly. This may require the involvement and collaboration of several departments within Grifols, as described in the relevant policies and procedures.

e. Keep personal data only for the period necessary for the purpose for which it is processed and as required by law. Employees shall only keep personal data in Grifols' files (both electronic and paper format) while it is needed to fulfil the purposes for which the personal data is being processed or if legally necessary. Employees shall take all reasonable steps to erase personal data when keeping it is no longer required. This may require the involvement and collaboration of several departments within Grifols, as described in the relevant policies and procedures.

f. Process personal data in a secure manner. Grifols shall adopt organisational and technical security measures to protect personal data, ensure its confidentiality, availability and if applicable, share them in a secure manner according to the regulations. All Grifols' employees are required to follow the applicable technical and organisational security measures, these measures are specially important whem processing special categories of personal data.

6.2. Data Subject Rights over their Personal Data

Data protection regulations confer individuals with several rights, including getting access to their personal data, having any erroneous personal data be corrected, or having their personal data erased, among others. These rights and how to exercise them are clearly stated in Grifols' privacy notices made available to individuals.

According to the applicable legislations, individual rights over their personal data could include the following:

- Information: the right to receive concise, transparent, intelligible and easily accessible information on the processing of personal data. In general, Grifols provides this information in privacy notices that include the contact details of the controller and the data protection officer, the purposes and

the legal basis (why) for the processing, the categories of recipients (if any), the retention period of the personal data and the data protection rights mentioned below, among others. The DPO and Grifols' legal advisors in collaboration with the employees will elaborate and/or revise privacy notices as needed.

- Access: the right to request confirmation as to whether or not personal data is being processed and, if so, to obtain access to personal data included in Grifols' files.
- Rectification: the right to request the modification of inaccurate personal data.
- Erasure: the right to request that personal data is erased.
- Objection: the right to request that personal data is not processed in specific circumstances.
- Portability: the right to request receipt, in an electronic file, of the personal data provided to Grifols, as well as the right to transmit this to other parties.
- Restriction of Processing: the right to request the restriction of personal data processing when:
  i. the accuracy of personal data is being verified after being contested;
  ii. the processing of personal data is unlawful and the data subject opposes its erasure;
  iii. Grifols no longer needs the personal data for the purposes of the processing, but it is required by the individual for the establishment, exercise or defence of legal claims, and
  iv. the data subject has objected to the processing based in the public interest or legitimate interest, whilst it is being verified whether the legitimate grounds of Grifols override those of the data subject.
- Withdrawal of Consent: right to withdraw the consent provided without affecting the lawfulness of processing based on consent provided before its withdrawal.

Grifols establishes internal procedures to facilitate and manage the exercise of individuals' data protection rights. Any Grifols' employee in receipt of a data subject rights request shall immediately contact the person or department in charge of data protection in their organization or in its abscence the Corporate Data Protection Office (privacy@grifols.com)

6.3. Personal Data Retention

When personal data is no longer needed for the purpose for which it is being processed or to comply with applicable legal obligations, employees shall take all reasonable steps to destroy or erase all copies of personal data, whether in paper or in any other physical or digital storage.

For further information on this topic, please refer to Grifols Data Retention Policy (ID448).

6.4. Personal Data Security and Data Breaches

Grifols puts in place procedures and technology to secure personal data throughout the period it is held, adopting reasonable technical and organisational measures to keep personal data secure, with a special focus on special categories of personal data. Grifols also establishes a process for regularly testing, assessing and evaluating the effectiveness of these measures, in order to ensure the:

a. Availability of personal data: business information systems and personal data can be used in the manner and time required. Grifols takes reasonable measures to protect against accidental or unauthorised loss, destruction, or damage by being able to promptly restore personal data in the event of a physical or technical incident.

b. Confidentiality of personal data: systems and files storing personal data are accessed only by duly authorized persons, preventing unauthorized, accidental or unlawful access or disclosure of personal data.

c. Integrity of personal data**:** to maintain the accuracy of personal data against accidental or fraudulent alteration.

All employees shall comply with the applicable Grifols' information security policies and procedures when processing personal data, including without limitation the IT Security Policy.

Personal data breaches are a type of security incident which compromises the availability, confidentiality or integrity of personal data. Grifols has designed procedures (DPO-SOP-000001_Personal Data Incident

Procedure) for employees to notify security incidents and personal data breaches, so that Grifols is in a position to carry out the corresponding risk and security assessment and to comply, if applicable, with its obligations to notify the data protection authority and the affected data subjects.

6.5. Personal Data Transfers and Service Providers

During the normal course of business, employees may need to contract a service and/or transfer personal data to Grifols' group companies or third parties in several countries for legitimate business reasons or as otherwise allowed or required by law.

When hiring a new service from a third party (whether from an existing vendor or a new one) that involve the processing of personal data, it is required to perform a vendor assessment to evaluate the risk and impact of that processing on data subjects' rights and freedoms. The purpose of the assessment is to confirm that the vendor has the capability to protect and process personal data in accordance with the principles and standards set forth in this policy and the provisions of the applicable data protection regulations.

All service agreements with third parties or Grifols' group companies that involve processing personal data have to include data protection clauses or a reference to an already executed data protection agreement.

Crossborder transfers of personal data are only acceptable if there are appropriate safeguards in place.

Grifols establishes internal procedures to verify that personal data transfers across borders and the contracting of service providers comply with the applicable data protection regulations.

6.6. Training and Awareness

Grifols seeks to foster a strong privacy culture within the company. Grifols promotes and provides appropriate training to its employees, proportional to the processing of personal data they do, with the objective to raise awareness and educate them on how to identify and deal with personal data, in a manner that complies with Grifols' standards and procedures, and the applicable privacy regulations.

6.7. Privacy by Design and Privacy by Default

Employees should consider privacy and data protection matters throughout the lifecycle of personal data (i.e. from collection to destruction) and shall therefore integrate data protection principles and security measures into their business activities within Grifols, in particular when implementing a new project. In addition, appropriate technical and organisational security measures shall be implemented to ensure that only strictly necesary required personal data is processed.

7. REASONS FOR CHANGE

Update of definitions and related documents.

GRIFOLS

Global Privacy and Data Protection Policy

FRENCH / FRANÇAIS

SOMMAIRE

1. OBJECTIF

La présente Politique de confidentialité et de protection des données (la « Politique ») vise à présenter les principes pertinents de protection des données suivis qui s'appliquent aux sociétés du Groupe Grifols (« Grifols ») pour la protection et la sécurité des données à caractère personnel et la façon dont ces principes sont appliqués.

Favoriser une culture de respect des données personnelles renforce les relations de confiance et contribue à la mission de Grifols d'améliorer la santé et le bien-être des personnes dans le monde entier.

2. CHAMP D'APPLICATION

La présente Politique s'applique à toutes les sociétés du Groupe Grifols (« Grifols ») sans préjudice des réglementations en matière de protection des données ou des lois locales applicables aux activités d'entreprise de Grifols, qui peuvent entraîner des dispositions plus ou moins strictes en matière de confidentialité et de protection des données que celles qui sont réglementées dans cette Politique. Par conséquent, les dispositions de cette Politique doivent être interprétées et appliquées conformément en œuvre conjointement avec les lois applicables.

Plus précisément, cette Politique s'applique à tous les employés de Grifols (les « employés ») qui traitent des données à caractère personnel dans le cadre des activités professionnelles menées par Grifols. Les données à caractère personnel sont toutes les informations qui permettent d'identifier une personne physique, soit directement, soit par l'association d'autres informations.

La présente Politique ne s'applique pas aux informations ou données qui ne sont pas des données à caractère personnel.

3. DOCUMENTS ASSOCIÉS

- *Code de conduit de Grifols*
- *Politique des droits de l'homme de Grifols*
- *Conditions générales mondiales pour les fournisseurs*
- *« Information Security Policy » (GHTI-CTRL-000237)*
- *« Information Technology Usage Policy » (CTRL-000110)*
- *Procédure relative aux incidents liés aux données à caractère personnel (DPO-SOP-000001)*
- *Politique de conservation des documents ("Records Retention Policy" ID448)*

Vous trouverez de plus amples informations sur la protection des données chez Grifols dans la section Data Protection Office de l'intranet.

4. DÉFINITIONS

Aux fins de la présente politique, les termes indiqués ci-dessous auront la signification suivante :

TERME	DÉFINITION
Consentement	Toute indication libre, spécifique, éclairée et sans ambiguïté de la volonté d'une personne par laquelle elle manifeste, par une déclaration ou par un acte positif clair, son accord pour le traitement des données à caractère personnel la concernant.
Responsable du traitement	Une personne physique ou morale, une autorité publique, une agence ou un autre organisme, qui détermine les finalités et les moyens du traitement des données à caractère personnel.

TERME	DÉFINITION
Corporate Data Protection Office	Département de l'entreprise chargé de soutenir les sociétés du groupe Grifols en matière de protection des données.
Réglementations sur la protection des données/confidentialité	Toute loi, réglementation, statut, acte, résolution, code, directive ou disposition, y compris ses amendements ou substitutions, relatifs à la vie privée ou au traitement des données à caractère personnel de personnes de tout pays du monde, applicable à Grifols, y compris, mais sans limitation, le RGPD.
Délégué à la protection des données (DPD)	Personne chargée d'informer, de conseiller et de contrôler la bonne conformité des questions relatives à la protection des données au sein de Grifols et qui agit également en tant qu'interlocuteur entre Grifols, les personnes concernées et l'Autorité de protection des données (APD) compétente.
Personne concernée / Personne physique	Toute personne dont les données à caractère personnel sont traitées par Grifols et qui peut être identifiée, directement ou indirectement, sur la base des données à caractère personnel disponibles (par ex. : employés, clients, donneurs, patients, etc.).
Règlement général sur la protection des données (RGPD)	Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données et abrogeant la directive 95/46/CE.
Données à caractère personnel / Informations personnelles	Toute information relative à une personne qui peut être identifiée ou qui est identifiable : - Directement à partir de ces informations (par ex. : nom, numéro d'identification, photo, etc.) - Indirectement à partir de ces informations et par l'association avec d'autres données (par ex. : dossiers médicaux, évaluation de la performance, adresse IP, etc.).
Incident/Violation des données à caractère personnel	Tout incident de sécurité qui entraîne la destruction, la perte, l'altération, la communication ou l'accès accidentels ou illégaux aux données personnelles transmises, stockées ou autrement traitées par Grifols ou par un tiers pour le compte de Grifols. Toutes les violations de données personnelles sont des incidents, mais tous les incidents ne sont pas nécessairement des violations de données personnelles.
Notice d'information	Document destiné aux personnes physiques contenant des informations sur le traitement des données à caractère personnel.
Traitement	Toute opération automatisée ou non automatisée impliquant des données à caractère personnel (par ex. : la collecte, l'enregistrement, le stockage, l'hébergement, la modification, la consultation, l'utilisation, la transmission de publications, l'effacement, etc.).
Catégories particulières de données à caractère personnel / Données à caractère personnel sensibles	Les données à caractère personnel considérées par la loi comme sensibles et nécessitant par conséquent un degré de protection plus élevé en raison de leur nature confidentielle et qui ne peuvent être traitées que dans des circonstances limitées.

TERME	DÉFINITION
	Voici quelques exemples : - Données relatives à l'origine raciale ou ethnique - Données relatives aux opinions politiques - Données relatives aux convictions religieuses ou philosophiques - Données relatives à l'affiliation syndicale - Données génétiques - Données biométriques traitées uniquement pour identifier un être humain - Données relatives à la santé - Données concernant la vie sexuelle ou l'orientation sexuelle - Données relatives à des condamnations et infractions pénales - Informations de santé protégées (Protected Health Information (PHI))
Autorité de contrôle / Autorité de protection des données (APD)	L'autorité publique indépendante responsable du contrôle et du respect de l'application des lois et réglementations en matière de protection des données. L'APD fournit également des conseils sur l'interprétation de la législation et, le cas échéant, impose des sanctions en cas de non-respect.
Tiers	Toute personne, physiques ou morales, autorités publiques, services ou organismes autres que le responsable du traitement, autorisés à traiter les données personnelles des personnes concernées, avec lesquelles interagit et qui n'est pas une société du groupe Grifols ou un employé.

5. RÔLES ET RESPONSABILITÉS

La protection de la vie privée et des données chez Grifols commence au niveau le plus haut, c'est-à-dire au niveau de la direction exécutive de l'entreprise. La protection de la vie privée et des données est l'un des principes du Code de conduite de Grifols et fait partie intégrante de notre culture et de nos activités d'entreprise. Par conséquent, elle concerne tout le monde au sein de l'entreprise.

Employés

Tous les employés de Grifols qui traitent des données à caractère personnel dans le cadre de leur activité professionnelle sont tenus de respecter cette politique. Les employés doivent contacter la personne ou le service responsable de la protection des données dans leur organisation ou, à défaut, le *Corporate Data Protection Office* (privacy@grifols.com) s'ils ont des questions sur l'application de celui-ci, ainsi que pour signaler toute violation potentielle de celle-ci.

Corporate Data Protection Office

Le *Corporate Data Protection Office*, Bureau de la protection des données de l'entreprise, est chargé de définir le cadre mondial de confidentialité de Grifols, ainsi que de superviser et de coordonner la conformité aux réglementations en matière de protection des données.

Elle collabore avec tous les départements et unités commerciales de Grifols pour renforcer le niveau de connaissances en matière de protection des données de tous les employés, en favorisant une culture de la confidentialité et en fournissant des solutions qui permettent une conformité opérationnelle avec les réglementations en matière de protection des données. L'objectif ultime est d'obtenir le respect du droit des personnes à la vie privée et la protection de leurs données personnelles.

Délégué à la protection des données

Pour les sociétés du groupe dans lesquelles un DPD a été nommé, celui-ci aura pour mission les fonctions suivantes :

- Informer, conseiller et surveiller le respect des réglementations applicables en matière de protection des données, y compris la sensibilisation et la formation du personnel impliqué dans les opérations de traitement des données.
- Fournir des conseils sur les analyses d'impact relatives à la protection des données et suivre leur mise en œuvre.
- Coopérer avec l'autorité de contrôle pour toutes les questions relatives au traitement des données personnelles.
- Agir en tant que point de contact pour l'autorité et les parties prenantes

Le DPD exerce ses fonctions dans le respect des risques liés aux opérations de traitement, en tenant compte de la nature, de la portée, du contexte et des finalités du traitement.

Département des technologies de l'information (TI)

Le service informatique est chargé de s'assurer de la mise en place de mesures de sécurité techniques et organisationnelles proportionnées au risque lié au traitement des données personnelles, conformément à l'ensemble des principes énoncés dans la présente politique.

6. POLITIQUE

La plupart des activités menées par Grifols impliquent le traitement des données personnelles de diverses parties prenantes, notamment les employés, les patients, les professionnels de la santé, les clients, les investisseurs, les fournisseurs et les donateurs, entre autres.

Grifols respecte le droit à la vie privée des personnes qui lui confient leurs données personnelles et s'engage à se conformer à la réglementation applicable en matière de protection des données.

L'engagement de Grifols en faveur de la transparence, de l'intégrité et des principes détaillés ci-dessous va au-delà de la simple conformité réglementaire. Grifols favorise une culture de la vie privée et de la protection des données personnelles en sensibilisant les employés à ce qu'elles sont et à la manière de les protéger, ainsi qu'en adoptant une approche de confidentialité dès la conception et par défaut. De cette façon, Grifols génère des relations de confiance avec ses partenaires et atténue le risque de violations de la sécurité des données personnelles, avec les dommages économiques et de réputation qui en découlent, contribuant ainsi à la croissance durable à long terme de Grifols et à son engagement envers la société.

6.1. Principes de protection des données à caractère personnel

Tous les employés de Grifols traitant des données à caractère personnel sont liés par cette politique et doivent suivre les principes suivants :

a. Traiter les données à caractère personnel de manière licite, équitable et transparente. Les employés doivent toujours s'assurer que Grifols a une base juridique adéquate qui justifie le traitement des données à caractère personnel des personnes concernées. D'une manière générale, les bases juridiques sont définies dans les réglementations sur la protection des données et comprennent notamment le traitement des données à caractère personnel pour exécuter un contrat (par ex. un contrat de travail), pour se conformer aux obligations légales applicables (par ex. pour communiquer des données à caractère personnel aux autorités fiscales) ou en raison des intérêts légitimes de Grifols, dans la mesure où ceux-ci ne prévalent pas sur les droits et libertés des personnes concernées (par exemple, la prévention de la fraude). Comme indiqué dans les règlements applicable sur la protection des données, les personnes concernées doivent être informées au préalable de la manière dont leurs données à caractère personnel seront traitées, qui sera responsable du traitement de leurs données et à qui elles peuvent être communiquées, entre autres aspects.

b. Collecter des données à caractère personnel uniquement à des fins spécifiées, explicites et légitimes. Les employés sont autorisés à collecter des données à caractère personnel

uniquement à des fins spécifiques et explicites qui sont licites et ne peuvent pas utiliser les données à caractère personnel à des fins autres que celles communiquées aux personnes concernées. Les modifications apportées à la finalité du traitement doivent être communiquées à l'avance à la personne concernée et peuvent faire l'objet d'une base juridique différente, et il peut être nécessaire d'obtenir le consentement de la personne concernée.

c. Traiter uniquement les données à caractère personnel adéquates, pertinentes et dans les limites de ce qui est nécessaire au regard des finalités (minimisation des données). Les employés doivent traiter uniquement les données à caractère personnel minimales requises pour la finalité spécifique communiquée à la personne concernée. Si ces données ne sont pas nécessaires, elles ne doivent en aucun cas être demandées ou traitées.

d. Traiter uniquement les données à caractère personnel qui sont exactes et mises à jour. Les employés doivent tout mettre en œuvre afin de que les données à caractère personnel qu'ils traitent sont exactes et mises à jour tout au long du cycle de vie des informations (de la collecte à la destruction par ex.). Pour ce faire, les employés feront tout leur possible pour rectifier ou effacer rapidement les données à caractère personnel inexactes. Cela peut nécessiter la participation et la collaboration de plusieurs départements au sein de Grifols, comme décrit dans les politiques et procédures correspondantes.

e. Conserver les données à caractère personnel uniquement pendant la période nécessaire à la finalité pour laquelle elles sont traitées et aux obligations légales applicables. Les employés ne doivent conserver les données à caractère personnel dans les fichiers de Grifols (au format électronique et au format papier) que si elles sont nécessaires aux fins pour lesquelles elles sont traitées ou si elles sont légalement nécessaires. Les employés mettront tout en œuvre pour effacer les données à caractère personnel lorsqu'elles ne sont plus nécessaires. Cela peut nécessiter la participation et la collaboration de plusieurs départements au sein de Grifols, comme décrit dans les politiques et procédures correspondantes.

f. Traiter les données à caractère personnel de manière sécurisée. Grifols adoptera des mesures de sécurité techniques et organisationnelles pour protéger les données personnelles, assurer leur confidentialité, leur intégrité et leur disponibilité et, le cas échéant, les partager en toute sécurité et dans le respect de la réglementation. Tous les employés de Grifols doivent respecter les mesures de sécurité techniques et organisationnelles applicables, qui sont particulièrement importantes lors du traitement de catégories particulières de données personnelles.

6.2. Droits des personnes physiques sur leurs données à caractère personnel

Les réglementations en matière de protection des données confèrent aux personnes physiques plusieurs droits, leur permettant notamment d'accéder à leurs données à caractère personnel, de demander la correction de données à caractère personnel erronées ou de demander la suppression de leurs données, entre autres. Ces droits et la manière de les exercer sont clairement indiqués dans les notices d'information que Grifols met à la disposition des personnes physiques.

En fonction de la réglementation applicable, les droits des personnes concernées en ce qui concerne leurs données personnelles peuvent inclure les éléments suivants :

- Information : le droit de recevoir des informations concises, transparentes, intelligibles et facilement accessibles sur le traitement des données à caractère personnel. En général, Grifols fournit ces informations dans des notices d'information qui reprennent, entre autres, les coordonnées du responsable du traitement et du délégué à la protection des données, les finalités et la base légale (pourquoi) du traitement, les catégories de destinataires (le cas échéant), la durée de conservation des données à caractère personnel et les droits de protection des données mentionnés ci-dessous. Le DPD et les conseillers juridiques de Grifols élaboreront et/ou réviseront, en collaboration avec les employés, les notices d'information nécessaires.
- Accès : le droit de demander la confirmation du traitement ou non des données à caractère personnel et, dans l'affirmative, d'accéder aux données à caractère personnel figurant dans les fichiers de Grifols.
- Rectification : le droit de demander la modification des données à caractère personnel inexactes.

- Effacement : le droit de demander que les données à caractère personnel soient effacées.
- Opposition : le droit de demander que les données à caractère personnel ne soient pas traitées dans des circonstances précises.
- Portabilité : le droit de recevoir, dans un fichier informatique, des données à caractère personnel fournies à Grifols, ainsi que le droit de les transmettre à d'autres parties.
- Limitation du traitement : le droit de demander une limitation du traitement des données à caractère personnel lorsque :

  i. l'exactitude des données à caractère personnel est en cours de vérification après remise en cause de leur exactitude ;
  ii. le traitement des données à caractère personnel est illégal et que la personne concernée s'oppose à leur effacement ;
  iii. Grifols n'a plus besoin des données à caractère personnel aux fins du traitement, mais qu'elles sont requises par la personne concernée pour la constatation, l'exercice ou la défense de droits en justice, et
  iv. la personne concernée s'est opposée au traitement pour l'exécution d'une tâche effectuée dans l'intérêt public ou nécessaire aux fins d'un intérêt légitime, lorsqu'il s'avère que les intérêts légitimes de Grifols prévalent sur ceux de la personne concernée.

- Retrait du consentement : le droit de retirer le consentement accordé sans porter atteinte à la licéité du traitement fondé sur le consentement effectué avant le retrait de celui-ci.

Grifols établit des procédures internes pour faciliter et gérer l'exercice des droits de protection des données des personnes physiques. Tout employé de Grifols qui reçoit une demande de la part d'une personne physique souhaitant exercer ses droits doit contacter immédiatement la personne ou le service en charge de la protection des données dans son organisation ou, à défaut, le *Corporate Data Protection Office* (privacy@grifols.com).

6.3. Conservation des données à caractère personnel

Lorsque les données à caractère personnel ne sont plus nécessaires aux fins pour lesquelles elles sont traitées ou pour se conformer aux obligations légales applicables, les employés doivent tout mettre en œuvre pour détruire ou effacer toutes les copies des données à caractère personnel, que ce soit sur papier ou sur tout autre dispositif de stockage physique ou électronique.

Pour de plus amples informations à ce sujet, veuillez-vous reporter à la Politique de conservation des documents (*"Records Retention Policy"* ID448).

6.4. Sécurité et violations des données à caractère personnel

Grifols applique des procédures et des technologies pour protéger les données personnelles aussi longtemps qu'elle les conserve en adoptant des mesures techniques et organisationnelles raisonnables pour maintenir la sécurité des données personnelles, avec une attention particulière aux catégories spéciales de données personnelles. Grifols établit également un processus périodique de vérification, d'évaluation et d'évaluation de l'efficacité de ces mesures, afin de s'assurer que :

a. La disponibilité des données à caractère personnel : que les systèmes d'information professionnels et les données à caractère personnel puissent être utilisés de la manière opportune et au moment voulu. Grifols prend des mesures raisonnables pour protéger les données personnelles contre la perte, la destruction ou les dommages accidentels ou non autorisés, et pour être en mesure de restaurer rapidement les données à caractère personnel en cas d'incident physique ou technique.

b. Confidentialité des données à caractère personnel : seules des personnes dûment autorisées accèdent aux systèmes et fichiers qui hébergent les données personnelles, empêchant ainsi l'accès ou la communication non autorisés, accidentels ou illicites des données personnelles.

c. Intégrité des données à caractère personnel **:** afin de maintenir l'exactitude des données à caractère personnel contre toute altération accidentelle ou frauduleuse.

Tous les employés doivent se conformer aux politiques et procédures de sécurité de l'information applicables chez Grifols lors du traitement des données à caractère personnel, y compris, sans s'y limiter, la Politique de Sécurité informatique.

Les violations de données personnelles sont un type d'incident de sécurité qui compromet la disponibilité, la confidentialité ou l'intégrité des données personnelles. Grifols a conçu des procédures (DPO-SOP-000001_ Procédure relative aux incidents de données personnelles) permettant aux employés de signaler les incidents et les violations de sécurité des données personnelles en interne, afin que Grifols soit en mesure d'effectuer l'évaluation des risques et de la sécurité correspondante et de se conformer, le cas échéant, aux obligations de notification à l'autorité de protection des données et aux personnes concernées.

6.5. Transferts de données à caractère personnel et prestataires de services

Dans le cours normal des affaires, les employés peuvent avoir besoin de souscrire à un service et/ou de transférer des données à caractère personnel aux sociétés du groupe Grifols ou à des tiers dans plusieurs pays soit pour des raisons commerciales légitimes, soit pour d'autres raisons autorisées ou requises par la loi.

Lors de la souscription à un nouveau service auprès d'un tiers (qu'il s'agisse d'un fournisseur existant ou d'un nouveau fournisseur) qui implique le traitement de données à caractère personnel, une évaluation du fournisseur doit être effectuée, afin d'évaluer le risque et l'impact d'un tel traitement sur les droits et libertés des personnes concernées. L'objectif d'une telle évaluation est de confirmer que le fournisseur a la capacité de protéger et de traiter les données personnelles conformément aux principes et normes énoncés dans la présente politique et dans les dispositions de la réglementation applicable en matière de protection des données.

Tous les contrats de prestation conclus avec des tiers ou des sociétés du groupe Grifols qui impliquent le traitement de données à caractère personnel doivent comporter des clauses de protection des données ou faire référence à un accord de protection des données déjà établi.

Les transferts transfrontaliers de données à caractère personnel ne sont acceptables que s'il existe des garanties appropriées.

Grifols établit des procédures internes pour vérifier que les transferts transfrontaliers de données à caractère personnel et l'établissement de contrats avec les prestataires de services respectent les réglementations applicables en matière de protection des données.

6.6. Formation et sensibilisation

Grifols cherche à promouvoir une culture robuste de la confidentialité au sein de l'entreprise. Grifols encourage et fournit une formation appropriée à ses employés, proportionnelle au traitement des données à caractère personnel qu'ils effectuent, et qui vise à afin de les sensibiliser et de les former à l'identification et au traitement des données à caractère personnel d'une manière qui soit conforme aux normes et procédures de Grifols et aux réglementations applicables en matière de protection des données.

6.7. Protection des données dès la conception et protection des données par défaut

Les employés doivent tenir compte des questions de confidentialité et de protection des données tout au long du cycle de vie des données à caractère personnel (par ex. de la collecte à la destruction) et doivent donc intégrer les principes de protection des données et les mesures de sécurité dans leurs activités professionnelles au sein de Grifols, en particulier lors de la mise en place d'un nouveau projet. De plus, des mesures de sécurité techniques et organisationnelles appropriées doivent être mises en œuvre afin de garantir que seules les données à caractère personnel requises sont traitées par défaut.

7. RAISONS DU CHANGEMENT

Mettre à jour les définitions et les documents connexes.

GRIFOLS

Global Privacy and Data Protection Policy

GERMAN / DEUTSCH

INDEX

1. ZWECK

Der Zweck dieser Datenschutzrichtlinie (im Folgenden als „Richtlinie“ bezeichnet) besteht darin, die relevanten Datenschutzgrundsätze zu erläutern, die für Unternehmen der Grifols-Gruppe (im Folgenden als "Grifols" bezeichnet) zum Schutz und zur Sicherheit personenbezogener Daten gelten, und wie diese Grundsätze umgesetzt werden.

Die Förderung einer Kultur des Respekts vor personenbezogenen Daten stärkt die Vertrauensbeziehungen und trägt zur Mission von Grifols bei, die Gesundheit und das Wohlbefinden von Menschen auf der ganzen Welt zu verbessern.

2. UMFANG

Diese Richtlinie gilt für sämtliche Unternehmen der Grifols-Gruppe unbeschadet der Datenschutzbestimmungen oder der lokalen Gesetze, die auf ihre Geschäftstätigkeit anwendbar sind und die Bestimmungen zum Schutz der Privatsphäre und des Datenschutzes festlegen können, die mehr oder weniger streng sind als die in dieser Richtlinie geregelten. Die Bestimmungen dieser Richtlinie müssen in Übereinstimmung mit geltendem Recht ausgelegt und durchgesetzt werden.

Diese Richtlinie gilt insbesondere für alle Mitarbeiter von Grifols (die „Mitarbeiter“), die personenbezogene Daten im Rahmen der Geschäftstätigkeit von Grifols verarbeiten. Personenbezogene Daten sind alle Informationen, die entweder direkt oder in Kombination mit anderen Informationen die Identifizierung einer Person ermöglichen.

Diese Richtlinie gilt nicht für Informationen oder Daten, bei denen es sich nicht um personenbezogene Daten handelt.

3. DAZUGEHÖRIGE DOKUMENTE

- *Grifols Verhaltenskodex*
- *Menschenrechtspolitik von Grifols*
- *Globale Geschäftsbedingungen für Lieferanten*
- *Information Security Policy (GHTI-CTRL-000237)*
- *Information Technology Usage Policy (CTRL-000110)*
- *Verfahrens zum Umgang mit Vorfällen mit personenbezogenen Daten (DPO-SOP-000001)*
- *Richtlinie zur Aufbewahrung von Unterlagen (“Records Retention Policy” ID448)*

Weitere Informationen zum Datenschutz bei Grifols finden Sie im Intranet in der Rubrik "Data Protection Office".

4. DEFINITIONEN

Zum Zweck dieser Richtlinie haben die nachfolgend aufgeführten Begriffe die folgende Bedeutung:

BEGRIFF	DEFINITION
Einwilligung	Jede freiwillige für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist.
Verantwortlicher	Natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.

BEGRIFF	DEFINITION
Corporate Data Protection Office	Die Abteilung des Unternehmens, die für die Unterstützung der Unternehmen der Grifols-Gruppe in Fragen des Datenschutzes zuständig ist.
Datenschutz / Datenschutzvorschriften	Alle Gesetze, Vorschriften, Statuten, Erlässe, Verordnungen, Kodizes, Richtlinien oder Bestimmungen, einschließlich Änderungen oder Ersatzregelungen, in Bezug auf den Datenschutz oder die Verarbeitung personenbezogener Daten von Personen in einem beliebigen Land der Welt, denen Grifols unterliegt, einschließlich, aber nicht beschränkt auf die DSGVO.
Datenschutzbeauftragter (DPO)	Person, die mit der Unterrichtung, Beratung und Überwachung der korrekten Einhaltung datenschutzrechtlicher Vorschriften bei Datenschutzangelegenheiten innerhalb von Grifols beauftragt ist und auch als Kontaktstelle zwischen Grifols, den betroffenen Personen und der Datenschutzbehörde dient.
Betroffene Person / Person	Jede Person, deren personenbezogene Daten von Grifols verarbeitet werden und die auf der Grundlage der verfügbaren personenbezogenen Daten direkt oder indirekt identifiziert werden kann (z. B. Mitarbeiter, Kunden, Spender, Patienten usw.).
Datenschutz-Grundverordnung (DSGVO)	Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG.
Personenbezogene Daten	Alle Informationen, die sich auf eine identifizierte oder identifizierbare Person beziehen: - direkt durch Verweis auf diese Informationen (z. B. Name, ID-Nummer, Lichtbild usw.) - indirekt aus diesen Informationen, in Verbindung mit anderen Daten (z. B. Krankenakten, Leistungsbeurteilung, IP-Adresse usw.).
Vorfall / Verstoß gegen personenbezogene Daten	Jeder Sicherheitsvorfall, der zur versehentlichen oder unrechtmäßigen Vernichtung, zum Verlust, zur Veränderung, zur Offenlegung oder zum Zugriff auf personenbezogene Daten führt, die von Grifols oder einem Dritten im Auftrag von Grifols übertragen, gespeichert oder anderweitig verarbeitet werden. Alle Verletzungen des Schutzes personenbezogener Daten sind Vorfälle, aber nicht alle Vorfälle sind notwendigerweise Verletzungen des Schutzes personenbezogener Daten.
Datenschutzhinweis	An Personen gerichtetes Dokument, das Informationen über die Verarbeitung personenbezogener Daten enthält.
Verarbeitung	Jeder automatisierte oder nicht automatisierte Vorgang, der personenbezogene Daten beinhaltet, z.B. Erhebung, Aufzeichnung, Speicherung, Hosting, Änderung, Konsultation, Verwendung, Offenlegung durch Übermittlung, Löschung usw.).
Besondere Kategorien von personenbezogenen Daten / sensible Daten	Personenbezogene Daten, die gemäß anwendbarem Recht als sensibel gelten und daher aufgrund ihrer privaten Natur einen höheren Schutz verdienen und die nur unter bestimmten Umständen verarbeitet werden können. Nachstehend einige Beispiele: - Rassische oder ethnische Herkunft - Politische Meinungen

BEGRIFF	DEFINITION
	- Religiöse oder weltanschauliche Überzeugungen - Gewerkschaftszugehörigkeit - Genetische Daten - Biometrische Daten, die ausschließlich zur Identifizierung eines Menschen verarbeitet werden - Gesundheitsbezogene Daten - Daten zum Sexualleben oder zur sexuellen Orientierung - Strafrechtliche Verurteilungen und Straftaten - Geschützte Gesundheitsinformationen *("Protected Health Information*", PHI)
Aufsichtsbehörde / Datenschutzbehörde (DPA)	Unabhängige staatliche Stelle, die für die Überwachung und Durchsetzung der Anwendung von Datenschutzgesetzen zuständig ist. Die Datenschutzbehörde bietet auch eine Anleitung zur Auslegung der Rechtsvorschriften und verhängt gegebenenfalls Sanktionen für Verstöße.
Dritter	Eine natürliche oder juristische Person, Behörde, Einrichtung oder sonstige Stelle – mit Ausnahme des Auftragsverarbeiters - die zur Verarbeitung personenbezogener Daten von betroffenen Personen befugt ist, mit denen Grifols interagiert und die weder ein Unternehmen noch Mitarbeiter der Grifols-Gruppe sind.

5. ROLLEN UND VERANTWORTLICHKEITEN

Datenschutz beginnt bei Grifols schon auf der Ebene der Geschäftsleitung. Als einer der Grundsätze des Verhaltenskodex von Grifols ist der Datenschutz ein zentraler Bestandteil unserer Kultur und Geschäftstätigkeit und betrifft alle im Unternehmen tätigen Personen.

Mitarbeiter

Alle Mitarbeiter von Grifols, die im Rahmen ihrer beruflichen Tätigkeit personenbezogene Daten verarbeiten, sind verpflichtet, diese Richtlinie einzuhalten. Die Mitarbeiter sollten sich an die Person oder Abteilung wenden, die für den Datenschutz in ihrem Unternehmen verantwortlich ist, oder ersatzweise an das *Corporate Data Protection Office* (privacy@grifols.com), wenn sie Fragen zur Anwendung der RIchtlinie haben und einen möglichen Verstoß melden möchten.

Corporate Data Protection Office

Das *Corporate Data Protection Office* ist verantwortlich für die Festlegung des globalen Datenschutzrahmens von Grifols sowie für die Überwachung und Koordination der Einhaltung der Datenschutzbestimmungen.

Es arbeitet mit allen Abteilungen und Geschäftsbereichen von Grifols zusammen, um das Bewusstsein für Datenschutzthemen unter allen Mitarbeitern zu stärken, eine Datenschutzkultur zu fördern und Lösungen bereitzustellen, die die operative Einhaltung der Datenschutzbestimmungen ermöglichen. Oberstes Ziel ist die Achtung des Rechts der Menschen auf Privatsphäre und den Schutz ihrer personenbezogenen Daten.

Datenschutzbeauftragter (DSB)

Bei Konzerngesellschaften, in denen ein DSB ernannt wurde, ist er für die folgenden Funktionen verantwortlich:

- Information, Beratung und Überwachung der Einhaltung der geltenden Datenschutzbestimmungen, einschließlich Sensibilisierung und Schulung der an der Datenverarbeitung beteiligten Mitarbeiter.
- Beratung zu Datenschutz-Folgenabschätzungen und Überwachung ihrer Umsetzung.
- Zusammenarbeit mit der Aufsichtsbehörde in allen Fragen im Zusammenhang mit der Verarbeitung personenbezogener Daten.
- Zentraler Ansprechpartner für Behörden und Stakeholder

Der DSB nimmt seine Aufgaben unter gebührender Berücksichtigung der mit den Verarbeitungsvorgängen verbundenen Risiken unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung wahr.

Abteilung für Informationstechnologie (IT)

Die IT-Abteilung ist dafür verantwortlich sicherzustellen, dass technische und organisatorische Sicherheitsmaßnahmen getroffen werden, die dem mit der Verarbeitung personenbezogener Daten verbundenen Risiko entsprechen und zwar in Übereinstimmung mit allen in dieser Richtlinie dargelegten Grundsätzen.

6. POLICY

Die meisten der von Grifols ausgeführten Tätigkeiten beinhalten die Verarbeitung personenbezogener Daten einer Vielzahl von Interessengruppen, z.B. Mitarbeiter, Patienten, Angehörige der Gesundheitsberufe, Kunden, Investoren, Lieferanten und Spender.

Grifols achtet die Datenschutzrechte aller Personen, die dem Unternehmen ihre personenbezogenen Daten anvertrauen, und verpflichtet sich zur Einhaltung aller geltenden Datenschutzbestimmungen.

Das Engagement von Grifols für Transparenz, Integrität und die unten aufgeführten Grundsätze geht über die bloße Einhaltung gesetzlicher Vorschriften hinaus. Grifols fördert eine Kultur des Datenschutzes, indem das Bewusstsein der Mitarbeiter dafür gestärkt wird, was personenbezogene Daten sind und wie diese geschützt werden können. Dabei verfolgt Grifols einen Ansatz von Privacy-by-Design- und Default.

Auf diese Weise baut Grifols Vertrauensbeziehungen zu seinen Partnern auf und mindert das Risiko von Verstößen gegen die Sicherheit personenbezogener Daten mit den daraus resultierenden wirtschaftlichen und Reputationsschäden und trägt so zum langfristigen nachhaltigen Wachstum und Engagement von Grifols für die Gesellschaft bei.

6.1. Grundsätze zum Schutz personenbezogener Daten

Alle Mitarbeiter von Grifols, die personenbezogene Daten verarbeiten, unterliegen dieser Richtlinie und müssen die folgenden Grundsätze befolgen:

a. Personenbezogene Daten auf rechtmäßige, faire und transparente Weise zu verarbeiten. Die Mitarbeiter müssen jederzeit sicherstellen, dass Grifols über eine angemessene rechtliche Begründung für die Verarbeitung personenbezogener Daten natürlicher Personen verfügt. Die Rechtsgrundlagen sind in der Regel in den Datenschutzbestimmungen festgelegt und umfassen unter anderem die Verarbeitung personenbezogener Daten zur Erfüllung eines Vertrags (z. B. eines Arbeitsvertrags), die Erfüllung einer geltenden gesetzlichen Verpflichtung (z. B. Meldung personenbezogener Daten an die Steuerverwaltungen) oder die berechtigten Interessen von Grifols, sofern diese die Rechte und Freiheiten der betroffenen Personen nicht außer Kraft setzen (z. B. Betrugsprävention). Gemäß den Bestimmungen der geltenden Datenschutzbestimmungen müssen betroffene Personen unter anderem vorab darüber informiert werden, wie ihre personenbezogenen Daten verarbeitet werden, wer für die Verarbeitung ihrer Daten verantwortlich ist und an wen sie möglicherweise kommuniziert werden.

b. Erhebung personenbezogener Daten ausschließlich für festgelegte, eindeutige und legitime Zwecke. Mitarbeiter dürfen personenbezogene Daten nur zu bestimmten, eindeutigen und rechtmäßigen Zwecken erheben, und dürfen personenbezogene Daten nicht für andere als für die den betroffenen Personen offengelegten Zwecke verwenden. Änderungen des Zwecks der Verarbeitung müssen der betroffenen Person im Voraus mitgeteilt werden und müssen möglicherweise auf eine andere Rechtsgrundlage gestützt werden. Möglicherweise muss dazu auch eine Einwilligung von der betroffenen Person eingeholt werden.

c. Personenbezogene Daten nur zu verarbeiten, die angemessen, relevant und auf das für die Zwecke erforderliche Maß beschränkt sind (Datenminimierung). Die Mitarbeiter verarbeiten nur die personenbezogenen Daten, die für den konkreten Zweck, der der betroffenen Person mitgeteilt wurde, minimal erforderlich sind. Nicht erforderliche Daten dürfen weder erhoben noch gespeichert oder anderweitig verarbeitet werden.

d. Verarbeitung ausschließlich von personenbezogenen Daten, die sachlich richtig und auf dem neusten Stand sind. Mitarbeiter müssen alle angemessenen Maßnahmen ergreifen, um sicherzustellen, dass die von ihnen verarbeiteten personenbezogenen Daten während des gesamten Informationslebenszyklus (d. h. von der Erhebung bis zur Vernichtung) sachlich richtig und auf dem neusten Stand sind. In diesem Zusammenhang werden die Mitarbeiter alle zumutbaren Anstrengungen unternehmen, um unrichtige personenbezogene Daten unverzüglich zu berichtigen oder zu löschen. Dies kann die Einbeziehung und Zusammenarbeit mehrerer Abteilungen innerhalb von Grifols erfordern, wie dies in den entsprechenden Richtlinien und Verfahren beschrieben wird.

e. Bewahren Sie personenbezogene Daten nur so lange auf, wie es zur Erfüllung der Zwecke der Verarbeitung und der geltenden gesetzlichen Verpflichtungen erforderlich ist. Mitarbeiter bewahren personenbezogene Daten nur so lange in den Akten und Dateien von Grifols (sowohl in elektronischer als auch in Papierform) auf, wie dies zur Erfüllung der Zwecke erforderlich ist, für welche die personenbezogenen Daten verarbeitet werden, oder soweit dies gesetzlich erforderlich ist. Mitarbeiter ergreifen sämtliche angemessenen Maßnahmen zur Löschung personenbezogener Daten, wenn deren Aufbewahrung nicht länger erforderlich ist. Dies kann die Einbeziehung und Zusammenarbeit mehrerer Abteilungen innerhalb von Grifols erfordern, wie dies in den entsprechenden Richtlinien und Verfahren beschrieben wird.

f. Personenbezogene Daten sicher zu verarbeiten. Grifols wird technische und organisatorische Sicherheitsmaßnahmen ergreifen, um personenbezogene Daten zu schützen, ihre Vertraulichkeit, Integrität und Verfügbarkeit zu gewährleisten und sie gegebenenfalls sicher und in Übereinstimmung mit den Vorschriften weiterzugeben. Alle Mitarbeiter von Grifols sind verpflichtet, die geltenden technischen und organisatorischen Sicherheitsmaßnahmen zu beachten, die bei der Verarbeitung besonderer Kategorien personenbezogener Daten besonders wichtig sind.

6.2. Rechte natürlicher Personen an ihren personenbezogenen Daten

Datenschutzvorschriften gewähren Personen bestimmte Rechte, u. a. Auskunft über ihre personenbezogenen Daten, Berichtigung unrichtiger personenbezogener Daten oder Löschung ihrer personenbezogenen Daten. Diese Rechte und ihre Ausübung sind in den Grifols Datenschutzhinweisen, die den betroffenen Personen zur Verfügung gestellt werden, eindeutig beschrieben.

Abhängig von den geltenden Vorschriften können die Rechte der betroffenen Personen in Bezug auf ihre personenbezogenen Daten Folgendes umfassen:

- Informationen: das Recht zum Erhalt präziser, transparenter, verständlicher und leicht zugänglicher Informationen über die Verarbeitung personenbezogener Daten. Im Allgemeinen stellt Grifols diese Informationen in Datenschutzhinweisen zur Verfügung, die unter anderem die Kontaktdaten des Verantwortlichen und des Datenschutzbeauftragten, die Zwecke und die Rechtsgrundlage (warum) für die Verarbeitung, die Kategorien der Empfänger (soweit vorhanden), die Aufbewahrungsfrist der personenbezogenen Daten und die nachfolgend genannten Datenschutzrechte enthalten. Der Datenschutzbeauftragte und die Rechtsberater von Grifols werden in Zusammenarbeit mit den Mitarbeitern bei Bedarf Datenschutzhinweise weiter ausführen bzw. überarbeiten.
- Auskunft: das Recht, eine Bestätigung darüber zu verlangen, ob personenbezogene Daten verarbeitet werden und, ist dies der Fall, das Recht auf Auskunft über diese personenbezogenen Daten, die in Grifols Akten und Dateien aufgeführt sind.
- Berichtigung: das Recht, die Änderung unrichtiger personenbezogener Daten zu verlangen.
- Löschung: das Recht, die Löschung personenbezogener Daten zu verlangen.
- Widerspruch: das Recht, zu verlangen, dass personenbezogene Daten unter bestimmten Umständen nicht verarbeitet werden.
- Übertragbarkeit: das Recht, den Erhalt der von der betroffenen Person an Grifols bereitgestellten personenbezogenen Daten in einer elektronischen Datei zu verlangen, sowie das Recht, diese an andere Parteien zu übermitteln.
- Einschränkung der Verarbeitung: das Recht, eine Einschränkung der Verarbeitung personenbezogener Daten zu verlangen, wenn:
  i. die Richtigkeit der personenbezogenen Daten überprüft wird, nachdem ihre Richtigkeit bestritten wurde,

ii. die Verarbeitung personenbezogener Daten unrechtmäßig ist und die betroffene Person ihre Löschung ablehnt,
iii. Grifols die personenbezogenen Daten für die Zwecke der Verarbeitung nicht länger benötigt, die Person sie jedoch zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen benötigt, und
iv. die betroffene Person hat der Verarbeitung aufgrund eines berechtigten Interesses oder eines öffentlichen Interesses widersprochen, und zwar für die Zeit, die erforderlich ist, um zu überprüfen, ob die berechtigten Gründe von Grifols gegenüber denen der betroffenen Person überwiegen.

- Widerruf der Einwilligung: das Recht auf Widerruf der erteilten Einwilligung, ohne dass die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung berührt wird.

Grifols richtet interne Verfahren ein, um die Ausübung der Datenschutzrechte natürlicher Personen zu erleichtern und zu verwalten. Jeder Mitarbeiter von Grifols, der von einer betroffenen Person einen Antrag auf Ausübung seiner Rechte erhält, muss sich unverzüglich an die für den Datenschutz zuständige Person oder Abteilung in seiner Organisation oder, falls dies nicht der Fall ist, an das *Corporate Data Protection Office* (privacy@grifols.com) wenden.

6.3. Aufbewahrung personenbezogener Daten

Wenn die personenbezogenen Daten für den Zweck, für den sie verarbeitet werden, oder zur Erfüllung geltender gesetzlicher Verpflichtungen nicht mehr erforderlich sind, müssen die Mitarbeiter alle angemessenen Schritte unternehmen, um alle Kopien dieser personenbezogenen Daten, sei es in Papier-, phsysischer oder elektronischer Form, zu vernichten und/oder zu löschen.

Weitere Informationen zu diesem Thema finden Sie in der Richtlinie zur Aufbewahrung von Unterlagen von Grifols (*"Records Retention Policy"* ID448).

6.4. Sicherheit personenbezogener Daten und Datenschutzverletzung

Grifols setzt geeignete technische und Organisatorische Maßnahmen ein, um personenbezogene Daten, insbesondereder besondere Kategorien, während des Verarbeitungszeitraumes zu schützen, um die Sicherheit dieser zu gewährleisten. Grifols führt auch ein periodisches Verfahren zur Überprüfung, Beurteilung und Bewertung der Wirksamkeit dieser Maßnahmen ein, um sicherzustellen:

a. Verfügbarkeit personenbezogener Daten: dass die Informationssysteme und personenbezogenen Daten des Unternehmens in der erforderlichen Weise und Zeit zugänglich sind. Grifols ergreift angemessene Maßnahmen, um personenbezogene Daten vor versehentlichem oder unbefugtem Verlust, Zerstörung oder Änderungen zu schützen und personenbezogene Daten im Falle eines physischen oder technischen Vorfalls umgehend wiederherstellen zu können.

b. Vertraulichkeit personenbezogener Daten: dass nur ordnungsgemäß autorisierte Personen auf die Systeme und Dateien zugreifen, in denen personenbezogene Daten gespeichert sind, um den unbefugten, fahrlässigen oder unrechtmäßigen Zugriff oder die Weitergabe personenbezogener Daten zu verhindern.

c. Integrität personenbezogener Daten: um die Richtigkeit personenbezogener Daten durch den Schutz vor versehentlicher Änderung oder Fälschung zu gewährleisten.

Alle Mitarbeiter müssen die für die Verarbeitung personenbezogener Daten geltenden Informationssicherheitsrichtlinien und -verfahren von Grifols einhalten, einschließlich, aber nicht beschränkt auf die IT Security Policy.

Verletzungen des Schutzes personenbezogener Daten sind eine Art von Sicherheitsvorfällen, die die Verfügbarkeit, Vertraulichkeit oder Integrität personenbezogener Daten gefährden. Grifols hat Verfahren (DPO-SOP-000001_ Verfahren in Bezug auf Vorfälle mit personenbezogenen Daten) entwickelt, mit denen Mitarbeiter Vorfälle und Sicherheitsverletzungen im Zusammenhang mit personenbezogenen Daten intern melden können, damit Grifols in der Lage ist, die entsprechende Risiko- und

Sicherheitsbewertung durchzuführen und gegebenenfalls den Verpflichtungen zur Benachrichtigung der Datenschutzbehörde und der betroffenen Personen nachzukommen.

6.5. Übermittlung personenbezogener Daten und Dienstleister

Während des normalen Geschäftsverlaufs müssen Mitarbeiter unter Umständen aus berechtigten operativen Gründen oder soweit dies anderweitig gesetzlich zulässig oder vorgeschrieben ist bei Konzernunternehmen von Grifols oder Dritten in mehreren Ländern eine Dienstleistung beauftragen bzw. personenbezogene Daten an diese Konzernunternehmen oder Dritte übermitteln.

Wenn eine neue Dienstleistung von einem Dritten (unabhängig davon, ob es sich um einen bestehenden oder einen neuen Anbieter handelt) in Anspruch genommen wird, die die Verarbeitung personenbezogener Daten beinhaltet, muss eine Bewertung des Anbieters durchgeführt werden, um das Risiko und die Auswirkungen einer solchen Verarbeitung auf die Rechte und Freiheiten der betroffenen Personen zu bewerten. Der Zweck einer solchen Bewertung besteht darin, zu bestätigen, dass der Anbieter in der Lage ist, personenbezogene Daten in Übereinstimmung mit den in dieser Richtlinie festgelegten Grundsätzen und Standards sowie den Bestimmungen der geltenden Datenschutzbestimmungen zu schützen und zu verarbeiten.

Alle Dienstleistungsverträge mit Dritten oder mit Unternehmen der Grifols-Gruppe, die die Verarbeitung personenbezogener Daten beinhalten, müssen Datenschutzklauseln oder einen Verweis auf einen bereits abgeschlossenen Datenschutzvertrag enthalten.

Grenzüberschreitende Übermittlungen personenbezogener Daten sind nur dann zulässig, wenn angemessene Sicherheitsmaßnahmen vorhanden sind. Geeignete Sicherheitsmaßnahmen können u.a. Standardvertragsklauseln oder Binding Corporate Rules darstellen.

Grifols richtet interne Verfahren ein, um zu überprüfen, ob die Übermittlung personenbezogener Daten zwischen Ländern und die Beauftragung von Dienstleistern mit den geltenden Datenschutzbestimmungen übereinstimmen.

6.6. Schulung und Sensibilisierung

Grifols strebt danach, eine starke Kultur des Datenschutzes im Unternehmen zu fördern. Grifols fördert und bietet seinen Mitarbeitenden angemessene Schulungen an, die proportional zur Verarbeitung personenbezogener Daten sind, die sie durchführen. Ziel ist es, das Bewusstsein zu schärfen und sie darin zu schulen, wie sie personenbezogene Daten identifizieren und verarbeiten, in Übereinstimmung mit den Standards und Verfahren von Grifols sowie den geltenden Datenschutzvorschriften.

6.7. Privacy by Design and Privacy by Default

Die Mitarbeiter müssen Fragen des Datenschutzes während des gesamten Lebenszyklus personenbezogener Daten (d. h. von der Erhebung bis zur Vernichtung) berücksichtigen und daher Datenschutzgrundsätze und Sicherheitsmaßnahmen in alle beruflichen Aktivitäten integrieren, die sie bei Grifols ausüben, insbesondere bei der Umsetzung neuer Projekte. Darüber hinaus werden geeignete technische und organisatorische Sicherheitsmaßnahmen getroffen, um sicherzustellen, dass standardmäßig nur die personenbezogenen Daten verarbeitet werden, die für den jeweiligen Zweck unbedingt erforderlich sind.

7. ÄNDERUNGSGRÜNDE

Aktualisieren von Definitionen und zugehörigen Dokumenten.

GRIFOLS

Global Privacy and Data Protection Policy

ITALIAN / ITALIANO

INDICE

1. FINALITÀ

La presente policy di protezione dei dati personali (“policy") ha la finalità di spiegare i principi di confidenzialità che si applicano alle società del Gruppo Grifols ("Grifols") per la protezione e la sicurezza dei dati personali nonché la loro attuazione.

Promuovere una cultura del rispetto dei dati personali rafforza i rapporti di fiducia e contribuisce alla missione di Grifols di migliorare la salute e il benessere delle persone in tutto il mondo.

2. AMBITO DI APPLICAZIONE

La presente policy si applica a tutte le società del Gruppo Grifols ("Grifols"), fatte salve le normative in materia di protezione dei dati o le leggi locali applicabili alle attività commerciali di Grifols, che potrebbero comportare disposizioni più o meno severe in materia di privacy e protezione dei dati rispetto a quelle regolamentate nella presente policy. Di conseguenza, le disposizioni della presente policy devono essere interpretate e applicate congiuntamente alle leggi applicabili.

In particolare, questa policy si applica a tutti i dipendenti Grifols (i “dipendenti”) che trattano i dati personali nell’ambito delle attività commerciali svolte da Grifols. Per dati personali si intende qualsiasi informazione che direttamente o in combinazione con altre informazioni consenta l'identificazione di una persona.

La presente policy non si applica a informazioni o a dati che non siano dati personali.

3. DOCUMENTI CORRELATI

- *Codice di condotta di Grifols*
- *Politica sui diritti umani di Grifols*
- *Termini e condizioni globali per i fornitori*
- *Information Security Policy (GHTI-CTRL-000237)*
- *Information Technology Usage Policy (CTRL-000110)*
- *Procedura in caso di incidente relativo ai dati personali (DPO-SOP-000001)*
- *Policy di conservazione dei registri (“Records Retention Policy” ID448)*

Ulteriori informazioni sulla protezione dei dati presso Grifols sono disponibili nella sezione "Data Protection Office" dell'intranet.

4. DEFINIZIONI

Ai fini della presente policy, i termini di seguito indicati hanno il seguente significato:

TERMINE	DEFINIZIONE
Consenso	Qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell’interessato, con la quale lo stesso esprime il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento.
Titolare del trattamento	La persona fisica o giuridica, l’autorità pubblica, il servizio o altro organismo, che determina le finalità e i mezzi del trattamento dei dati personali.
Corporate Data Protection Office	Direzione aziendale incaricata di supportare le società del gruppo Grifols in materia di protezione dei dati.
Normative sulla Protezione dei Dati/Privacy	Qualsiasi legge, regolamento, statuto, atto, risoluzione, linea guida o disposizione, incluse le modifiche o le sostituzioni relative alla privacy o al trattamento dei dati personali di persone in qualsiasi paese del mondo applicabili a Grifols incluso, a titolo non esaustivo, il GDPR.

TERMINE	DEFINIZIONE
Responsabile della protezione dei dati (DPO)	La persona incaricata di informare, consigliare e monitorare la corretta conformità delle questioni relative alla protezione dei dati all'interno di Grifols e che funge anche da punto di contatto tra Grifols, gli interessati e l'Autorità di protezione dei dati (DPA) competente.
L'Interessato /Persona fisica	Qualsiasi persona i cui dati personali sono trattati da Grifols e che può essere identificata, direttamente o indirettamente, sulla base di tali dati personali disponibili (ad es. dipendenti, clienti, donatori, pazienti, ecc.).
Regolamento generale sulla protezione dei dati (GDPR)	Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, e che abroga la direttiva 95/46/CE.
Dati o informazioni personali	Qualsiasi informazione riguardante una persona fisica («interessato») identificata o identificabile: - Direttamente con riferimento a tali informazioni (per es. nome, numero di C.I., foto, ecc.) - Indirettamente da tali informazioni in combinazione con altri dati (ad es. cartelle sanitarie, valutazione delle prestazioni, indirizzo IP, ecc.).
Violazione dei dati personali	Qualsiasi incidente di sicurezza che provochi la distruzione, la perdita, l'alterazione, la comunicazione o l'accesso accidentale o illecito ai dati personali trasmessi, archiviati o altrimenti trattati da Grifols o da terzi per conto di Grifols. Tutte le violazioni dei dati personali sono incidenti, ma non tutti gli incidenti sono necessariamente violazioni dei dati personali.
Informativa sulla privacy	Documento indirizzato ai singoli soggetti contenente informazioni sul trattamento dei dati personali.
Trattamento	Qualsiasi operazione automatizzata o non automatizzata che riguardi i dati personali (ad es. raccolta, registrazione, archiviazione, hosting, modifica, consultazione, utilizzo, trasmissione di pubblicazioni, cancellazione, ecc.).
Categorie speciali di dati personali / Dati personali sensibili	I dati personali considerati sensibili dalla legge e pertanto che richiedono una maggiore protezione per la loro natura privata e che possono essere trattati solo in circostanze limitate. Si riportano nel seguito alcuni esempi: - Origini razziali o etniche - Opinioni politiche - Convinzioni religiose o filosofiche - Appartenenza a sindacati - Dati genetici - Dati biometrici trattati esclusivamente per identificare un essere umano - Dati relativi alla salute - Dati riguardanti la vita sessuale o l'orientamento sessuale - Condanne e reati penali - Informazioni sanitarie protette (*Protected Health Information,* PHI)
Autorità di controllo / Autorità di protezione dei dati (DPA)	Autorità pubblica indipendente responsabile del monitoraggio e dell'applicazione delle leggi e dei regolamenti sulla protezione dei dati. L'autorità di protezione dei dati fornisce inoltre un orientamento sull'interpretazione della normativa e, se del caso, impone sanzioni per l'inosservanza della stessa.
Terzi	Persone fisiche o giuridiche, autorità pubbliche, servizi o organismi diversi dal titolare del trattamento, autorizzati al trattamento dei dati personali degli

TERMINE	DEFINIZIONE
	interessati, con i quali Grifols interagisce e che non sono società o dipendenti di Grifols.

5. RUOLI E RESPONSABILITÀ

La protezione dei dati e della vita privata presso Grifols inizia dall'alto, sotto la guida della Direzione. Essendo uno dei princìpi del Codice di condotta di Grifols,è è parte integrante della nostra cultura e delle nostre attività commerciali e riguarda tutti coloro che operano in azienda.

I dipendenti

Tutti i dipendenti di Grifols che trattano dati personali nell'ambito della loro attività professionale sono tenuti a rispettare la presente policy. Per eventuali domande relative alla sua applicazione nonché per segnalare qualsiasi potenziale violazione della stessa, i dipendenti devono contattare la persona o il dipartimento responsabile della protezione dei dati nella loro organizzazione o, in mancanza, la *Corporate Data Protection Office* (privacy@grifols.com).

Corporate Data Protection Office

La Corporate Data Protection Office è incaricata di definire il quadro globale della privacy di Grifols, oltre a supervisionare e coordinare il rispetto delle normative sulla protezione dei dati.

Collabora con tutti i dipartimenti e le business unit di Grifols per rafforzare il livello di conoscenza in materia di protezione dei dati tra tutti i dipendenti, promuovendo una cultura della privacy e fornendo soluzioni che consentano il rispetto operativo delle normative sulla protezione dei dati. L'obiettivo finale è quello di raggiungere il rispetto del diritto delle persone alla privacy e alla protezione dei loro dati personali.

Il responsabile della protezione dei dati (DPO)

Per le società del gruppo in cui è stato nominato un DPO, questi sarà responsabile delle seguenti funzioni:

- Informare, consigliare e monitorare il rispetto delle normative applicabili in materia di protezione dei dati, compresa la sensibilizzazione e la formazione del personale coinvolto nelle operazioni di trattamento dei dati.
- Fornire consulenza sulle valutazioni d'impatto sulla protezione dei dati e monitorarne l'attuazione.
- Collaborare con l'autorità di controllo in tutte le questioni relative al trattamento dei dati personali.
- Fungere da punto di contatto per l'autorità e le parti interessate

Il DPO svolge le sue funzioni tenendo in debita considerazione i rischi associati alle operazioni di trattamento, tenendo conto della natura, dell'ambito, del contesto e delle finalità del trattamento.

Dipartimento di Tecnologie dell'Informazione (IT)

Il dipartimento IT ha la responsabilità di garantire che siano in atto misure di sicurezza tecniche e organizzative commisurate al rischio associato al trattamento dei dati personali, in conformità con tutti i principi stabiliti nella presente policy.

6. POLICY

La maggior parte delle attività svolte da Grifols prevede il trattamento dei dati personali di varie categorie di Interessati, tra cui, a titolo esemplificativo e non esaustivo, dipendenti, pazienti, operatori sanitari, clienti, investitori, fornitori e donatori.

Grifols rispetta il diritto alla privacy delle persone che gli affidano i propri dati personali e si impegna a rispettare le normative applicabili in materia di protezione dei dati.

L'impegno di Grifols per la trasparenza, l'integrità e i principi descritti di seguito va oltre la mera conformità normativa. Grifols promuove una cultura della privacy e della protezione dei dati personali sensibilizzando i dipendenti su cosa sono e come proteggerli, nonché adottando un approccio privacy-by-design e privacy by default. In questo modo, Grifols genera relazioni di fiducia con i propri partner e mitiga il rischio di violazioni della sicurezza dei dati personali, con i conseguenti danni economici e reputazionali,

contribuendo così alla crescita sostenibile e all'impegno a lungo termine di Grifols nei confronti della società.

6.1. Principi di protezione dei dati personali

Tutti i dipendenti di Grifols che trattano dati personali sono soggetti a questa policy e devono seguire i seguenti principi:

a. Elaborare i dati personali in modo lecito, equo e trasparente. I dipendenti devono sempre accertarsi che la Grifols abbia una giustificazione legale adeguata per trattare i dati personali delle persone. In generale, le basi giuridiche sono stabilite nei regolamenti sulla protezione dei dati e questi includono, a titolo esemplificativo, il trattamento dei dati personali ai fini dell'esecuzione di un contratto (ad es. un contratto di lavoro), l'adempimento degli obblighi di legge applicabili (ad es. la comunicazione dei dati personali alle autorità fiscali) o a causa di legittimi interessi di Grifols, a condizione che questi non prevalgano sui diritti e le libertà degli interessati (ad es. prevenzione delle frodi). Come stabilito nei regolamenti sulla protezione dei dati applicabili, gli interessati devono essere informati in anticipo sulle modalità di trattamento dei loro dati personali, su chi detiene i loro dati e a chi possono essere comunicati, tra gli altri aspetti.

b. Raccogliere i dati personali esclusivamente per scopi specifici, espliciti e legittimi. Ai dipendenti è consentito raccogliere dati personali solo per finalità specifiche, esplicite e lecite e non possono utilizzare i dati personali per finalità diverse da quelle comunicate agli interessati. Le modifiche alle finalità del trattamento devono essere comunicate all'interessato in anticipo e potrebbero richiedere una motivazione giuridica diversa e il consenso dell'interessato.

c. Trattare solo dati personali adeguati, pertinenti e limitati a quanto necessario in relazione alle finalità (minimizzazione dei dati). I dipendenti potranno trattare solamente i dati personali minimi richiesti per le specifiche finalità comunicate all'interessato. Se i dati personali o certi tipi di dati personali non sono necessari, non devono essere richiesti o trattati in alcun modo.

d. Trattare solamente dati personali corretti e aggiornati. I dipendenti devono adottare tutte le misure ragionevoli per garantire che i dati personali da loro trattati siano corretti e aggiornati durante il ciclo di vita delle informazioni (ovvero, dalla raccolta alla distruzione). A tale riguardo, i dipendenti faranno quanto ragionevolmente possibile per rettificare o cancellare tempestivamente i dati personali inesatti. Ciò può richiedere il coinvolgimento e la collaborazione di diverse funzioni all'interno di Grifols, come descritto nelle relative policy e procedure.

e. Conservare i dati personali solo per il periodo necessario a rispettare le finalità del trattamento e gli obblighi di legge applicabili. I dipendenti conserveranno i dati personali solamente negli archivi di Grifols (sia in formato elettronico che cartaceo) per il tempo necessario a soddisfare le finalità per le quali i dati personali sono trattati o se richiesto dalla legge. I dipendenti devono adottare tutte le misure ragionevoli per cancellare i dati personali quando non sono più necessari. Ciò può richiedere il coinvolgimento e la collaborazione di diverse funzioni all'interno di Grifols, come descritto nelle relative policy e procedure.

f. Trattare i dati personali in modo sicuro. Grifols adotterà misure di sicurezza tecniche e organizzative per proteggere i dati personali, garantirne la riservatezza, l'integrità e la disponibilità e, se applicabile, condividerli in modo sicuro e nel rispetto delle normative. Tutti i dipendenti di Grifols devono osservare le misure di sicurezza tecniche e organizzative applicabili, che sono particolarmente importanti nel trattamento di categorie particolari di dati personali.

6.2. Diritti delle persone fisiche sui loro dati personali

Le norme sulla protezione dei dati conferiscono alle persone diversi diritti, tra cui l'accesso ai propri dati personali, la correzione di eventuali dati personali errati o la cancellazione dei propri dati personali ed altri diritti. Tali diritti e le modalità in cui possono essere esercitati sono chiaramente indicati nell'informativa sulla privacy di Grifols messa a disposizione delle persone.

A seconda della normativa applicabile, i diritti degli interessati in relazione ai propri dati personali possono includere quanto segue:

- Informazioni: il diritto di ricevere informazioni concise, trasparenti, intelligibili e facilmente accessibili sul trattamento dei dati personali. In generale, Grifols fornisce queste informazioni nell'informativa sulla privacy che comprende, tra gli altri, i dati di contatto del titolare e del responsabile della protezione dei dati, le finalità e la base giuridica (perché) per il trattamento, le categorie di destinatari (se esistenti), il periodo di conservazione dei dati personali e i diritti di protezione dei dati di seguito citati. I consulenti legali e il DPO di Grifols in collaborazione con i dipendenti elaboreranno e/o rivedranno l'informativa sulla privacy secondo necessità.
- Accesso: il diritto di richiedere conferma in merito all'eventuale trattamento dei dati personali e, in caso affermativo, di ottenere l'accesso ai dati personali inseriti nei file di Grifols.
- Rettifica: il diritto di richiedere la modifica di dati personali inesatti.
- Cancellazione: il diritto di richiedere la cancellazione dei dati personali.
- Obiezione: il diritto di richiedere che i dati personali non siano trattati in circostanze specifiche.
- Portabilità: il diritto di richiedere la ricezione, su supporto elettronico, dei dati personali forniti a Grifols, nonché il diritto di trasmetterli ad altri soggetti.
- Limitazione del trattamento: il diritto di richiedere una limitazione delle modalità di trattamento dei dati personali quando:

    i. dopo la contestazione della correttezza dei dati personali, è necessario verificarne la correttezza;
    ii. il trattamento dei dati personali è illecito e l'interessato si oppone alla loro cancellazione;
    iii. Grifols non ha più bisogno dei dati personali per le finalità del trattamento, ma la persona ne ha bisogno per l'istituzione, l'esercizio o la difesa di azioni legali, e
    iv. l'interessato si è opposto al trattamento basato sul legittimo interesse o sull'interesse pubblico, per il tempo necessario a verificare se i motivi legittimi di Grifols prevalgano su quelli dell'interessato.

- Revoca del consenso: La revoca del consenso non pregiudica la liceità del trattamento basata sul consenso prima della revoca.

Grifols stabilisce procedure interne per facilitare e gestire l'esercizio dei diritti di protezione dei dati delle persone fisiche. Qualsiasi dipendente di Grifols che riceva una richiesta da parte di un interessato di esercitare i propri diritti deve contattare immediatamente la persona o il dipartimento responsabile della protezione dei dati nella propria organizzazione o, in mancanza, la *Corporate Data Protection Office* (privacy@grifols.com).

6.3. Conservazione dei dati personali

Quando i dati personali non sono più necessari per lo scopo per il quale sono trattati o per adempiere agli obblighi di legge applicabili, i dipendenti adotteranno tutte le misure ragionevoli per distruggere o cancellare tutte le copie dei dati personali, sia in formato cartaceo che in qualsiasi altro supporto di conservazione fisica o elettronica.

Per ulteriori informazioni sull'argomento, si prega di consultare la policy di conservazione dei dati di Grifols (*"Records Retention Policy"* ID448).

6.4. Sicurezza dei dati personali e violazioni della sicurezza

Grifols applica procedure e tecnologie per proteggere i dati personali per tutto il tempo in cui li conserva, adottando misure tecniche e organizzative ragionevoli per mantenere la sicurezza dei dati personali, con particolare attenzione alle categorie speciali di dati personali. Grifols stabilisce inoltre un processo periodico di controllo e di valutazione dell'efficacia di tali misure, al fine di garantire che:

a. Disponibilità dei dati personali: che i sistemi informativi e i dati personali dell'azienda siano accessibili nei modi e nei tempi richiesti. Grifols adotta misure ragionevoli per proteggere i dati personali da perdita, distruzione o danni accidentali o non autorizzati e per essere in grado di ripristinare tempestivamente i dati personali in caso di incidente fisico o tecnico.

b. Riservatezza dei dati personali: che solo le persone debitamente autorizzate accedano ai sistemi e agli archivi che ospitano i dati personali, impedendo l'accesso o la comunicazione non autorizzati, accidentali o illeciti dei dati personali.

c. Integrità dei dati personali**:** per mantenere l'accuratezza dei dati personali contro qualsiasi alterazione accidentale o fraudolenta.

Tutti i dipendenti devono rispettare le policy e le procedure applicabili in materia di sicurezza delle informazioni della Grifols nel trattamento dei dati personali, ivi inclusi, a titolo non esaustivo, la Policy di sicurezza informatica.

Le violazioni dei dati personali sono un tipo di incidente di sicurezza che mette a rischio la disponibilità, la riservatezza o l'integrità dei dati personali. Grifols ha progettato procedure (DPO-SOP-000001_ Procedura in caso di incidente relativo ai dati personali) per consentire ai dipendenti di segnalare internamente incidenti e violazioni della sicurezza dei dati personali, in modo che Grifols sia in grado di effettuare la corrispondente valutazione del rischio e della sicurezza e di rispettare, se del caso, gli obblighi di notifica all'autorità per la protezione dei dati e agli interessati.

6.5. Trasferimenti di dati personali e fornitori di servizi

Durante il normale svolgimento dell'attività, i dipendenti potrebbero dover sottoscrivere un servizio e/o trasferire dati personali a società del gruppo Grifols o a terzi in diversi paesi per legittimi motivi aziendali o come altrimenti consentito o richiesto dalla legge.

Quando un nuovo servizio viene appaltato a una terza parte (sia essa un fornitore esistente o nuovo) che comporta il trattamento di dati personali, deve essere effettuata una valutazione del fornitore per valutare il rischio e l'impatto di tale trattamento sui diritti e sulle libertà degli interessati. Lo scopo di tale valutazione è quello di confermare che il fornitore ha la capacità di proteggere e trattare i dati personali in conformità con i principi e gli standard stabiliti nella presente policy e nelle disposizioni delle normative applicabili in materia di protezione dei dati.

Tutti i contratti di servizio con terzi o con società del gruppo Grifols che comportano il trattamento di dati personali devono includere clausole di protezione dei dati o un riferimento a un contratto di protezione dei dati già formalizzato.

I trasferimenti transfrontalieri di dati personali saranno accettabili solo se sono in atto garanzie adeguate.

Grifols stabilisce procedure interne per verificare che i trasferimenti di dati personali tra paesi e la contrattazione di fornitori di servizi siano conformi alle normative applicabili in materia di protezione dei dati.

6.6. Formazione e sensibilizzazione

Grifols cerca di promuovere una forte cultura della privacy in azienda. A tal fine, promuove e fornisce ai propri dipendenti una formazione adeguata, proporzionata al trattamento dei dati personali che effettuano e che mira a sensibilizzare ed educare su come identificare e trattare i dati personali in modo conforme alle norme e alle procedure di Grifols e alle normative applicabili in materia di protezione dei dati.

6.7. Privacy by design e privacy by default

I dipendenti devono tener conto delle questioni relative alla privacy e alla protezione dei dati per tutto il ciclo di vita dei dati personali (cioè dalla raccolta alla distruzione) e devono pertanto integrare i principi di protezione dei dati e le misure di sicurezza nella propria attività lavorativa all'interno dell'azienda, in particolare quando viene avviato un nuovo progetto. Inoltre, saranno implementate adeguate misure di sicurezza tecniche e organizzative atte a garantire che di default siano trattati solo i dati personali strettamente necessari per ciascuna finalità. .

7. MOTIVI DEL CAMBIAMENTO

Aggiornamento delle definizioni e dei relativi documenti.

GRIFOLS

Global Privacy and Data Protection Policy

JAPANESE / 日本語

目次

1. 目的

本プライバシーおよびデータ保護方針（以下「本方針」）は、Grifols グループ全社（「Grifols」）における個人データの保護およびセキュリティに関して適用される関連するプライバシー原則を説明し、この原則の実施方法を明示することを目的としています。

個人データに対する尊重の文化を醸成することは、信頼関係を強化し、世界中の人々の健康と福祉の向上を目指す Grifols の使命に寄与するものです。

2. 適用範囲

本方針は、Grifols グループ全社に適用されますが、各事業活動に適用されるデータ保護規制や現地法令に影響を与えるものではありません。これらの法規は、本方針に定めるプライバシーおよびデータ保護の要件よりも厳格または緩和された規定を設けている場合があります。したがって、本方針の規定は、適用法令と併せて解釈、実施されるべきものとします。

特に、本方針は、Grifols が行う事業活動の一環として個人データを取り扱う全従業員（以下「従業員」）に適用されます。個人データとは、単独または他の情報と組み合わせることで個人を特定できる情報を指します。

なお、本方針は、個人データに該当しない情報またはデータには適用されません。

3. 関連文書

- *Grifols の行動規範*
- *Grifols の人権方針*
- *ベンダー向けグローバル取引条件*
- *情報セキュリティ方針 - "Information Security Policy"（GHTI-CTRL-000237）*
- *情報技術利用方針 - "Information Technology Usage Policy"（CTRL-000110）*
- *個人データインシデント手順書（DPO-SOP-000001）*
- *記録保存方針 - "Records Retention Policy"（ID448）*

Grifols のプライバシーに関する詳細は、イントラネット内の Data Protection Office セクションを参照してください。

4. 定義

本方針において使用される用語は、以下の意味を有するものとします。

用語	定義
同意	本人が自身に関する個人データの処理に同意していることを、明示的な意思表示または明確な肯定的行動によって示す、自発的で、特定され、十分に情報提供され、かつ曖昧さのない意思表示。
管理者	個人データの処理の目的および手段を決定する自然人または法人、公的機関、団体、その他の組織体。
„Corporate Data Protection Office"	Grifols グループ各社をデータ保護において支援するコーポレート部門。
データ保護／プライバシー関連規制	Grifols に適用される、世界各国におけるプライバシーまたは個人データの処理に関する、あらゆる法律、規則、法令、制定法、決議、規範、指針、その他の規定（その改正または代替を含む）。なお、これには一般データ保護規制（GDPR）を含み、これに限定されません。

用語	定義
データ保護責任者 – *"Data Protection Officer"*（DPO）	Grifols におけるデータ保護関連事項の適正な順守を周知・助言・監督する役割を担い、あわせて、Grifols とデータ主体および所管のデータ保護監督機関（DPA）との連絡窓口として指定された自然人または法人。
データ主体／本人	Grifols により処理される個人データの対象となる、直接的または間接的に識別可能な自然人（例：従業員、顧客、ドナー、患者など）。
一般データ保護規制 – *„General Data Protection Regulation"*（GDPR）	個人データの処理に関する自然人の保護および当該データの自由な移動に関する 2016 年 4 月 27 日付欧州議会および理事会規制（EU）2016/679、ならびに指令 95/46/EC の廃止。
個人データ／個人情報	識別された、または識別可能な個人に関連するすべての情報： –該当情報自体によって直接的に個人を識別できる場合（例：氏名、ID 番号、写真など） –該当情報と他の情報を組み合わせることで間接的に個人を識別できる場合（例：健康記録、業績評価、IP アドレスなど）。
個人データ漏えい／インシデント	Grifols または Grifols に代わって第三者機関による個人データの送信・保管・処理において、偶発的または違法な破壊、喪失、改ざん、漏えい、アクセスが発生するセキュリティインシデント。すべての個人データ漏えいはインシデントに該当しますが、その逆は必ずしも該当しません。
プライバシー通知	個人データの処理に関する情報を本人に伝える文書。
処理	個人データに関して自動・非自動を問わず行われるあらゆる操作（例：収集、記録、保存、修正、使用、送信、削除など）。
要配慮個人データ／機微な個人データ	法律上、機微な情報と見なされ、その性質上、より高いレベルの保護が求められる個人データであり、限定された条件下でのみ処理が許可されるもの。以下はその一例です。 人種や民族についての情報 政治的な意見や考え方 宗教や人生観などの信念 労働組合への加入状況 遺伝子に関する情報 顔認証や指紋など、本人確認のためのデータ 健康状態や病歴などの情報 性的指向や性生活に関する情報 犯罪歴や違法行為に関する記録 医療機関が保護すべき健康情報（*Protected Health Information* PHI）
監督機関／データ保護機関（DPA）	データ保護に関する法令および規制の適用状況を監視・執行する責任を有する、独立した公的機関。DPA は、関連法令の解釈に関する指針を提供し、必要に応じて違反に対して制裁を科す権限も有します。
第三者機関	Grifols と関係を有し、かつ Grifols グループ会社または従業員ではない、個人データの処理を許可された処理者以外の自然人または法人、公的機関、団体、またはその他の組織体。

5. 役割と責任

Grifols におけるプライバシーおよびデータ保護は、経営幹部の主導のもと、最上層から始まります。Grifols 行動規範の原則の一つとして、本事項は当社の企業文化および事業活動に不可欠な要素であり、社内のすべての者に関わるものです。

従業員

職務上、個人データを取り扱う Grifols の全従業員には、本方針を遵守する義務があります。本方針の適用に関して疑問がある場合や、違反の可能性を認識した場合は、所属組織のプライバシー担当者または *Corporate Data Protection Office*（privacy@grifols.com）に連絡してください。

Corporate Data Protection Office

Corporate Data Protection Office は、Grifols 全体のプライバシー体制を構築・管理し、データ保護規制への対応状況を確認・調整する役割を担っています。

Grifols の全部門および事業部門と協力し、全従業員のデータ保護に関する意識を高め、プライバシー文化を醸成し、プライバシー関連規制を遵守するためのソリューションを提供しています。その究極の目的は、人々のプライバシーおよび個人データ保護の権利を守ることです。

データ保護責任者（DPO）

DPO が任命されているグループ会社においては、以下の職務を担います。

- 関連するデータ保護規制の順守状況について、情報提供、助言および監視を行うこと（処理業務に関与する職員への意識向上および研修も含む）。
- データ保護影響評価に関する助言を提供し、その実施状況を監督すること。
- 個人データの処理に関するすべての事項において監督機関と協力すること。
- 監督機関および関係者との連絡窓口としての機能を果たすこと

DPO は、処理業務に関わるリスクを十分に考慮し、その性質、範囲、文脈および目的に応じて、適切に職務を遂行するものとします。

情報技術部門（Information Technology Department）

IT 部門は、本方針に記載された原則に従い、個人データの処理に伴うリスクに応じた技術的および組織的なセキュリティ対策を実施する責任を負います。

6. 方針

Grifols が行うほぼすべての活動には、従業員、患者、医療従事者、顧客、投資家、ベンダー、ドナーなど、さまざまな関係者の個人データの処理が伴います。

Grifols は、個人データを提供してくれるすべての方々のプライバシー権を尊重し、適用されるすべてのプライバシー関連規制を遵守することを約束します。　.

Grifols は、透明性、完全性および本文書に記載された原則を、単なる法令遵守を超えて重視しており、プライバシー保護を企業文化の一部として推進しています。従業員に対し個人データとは何か、またどのように保護すべきかを啓発するとともに、「設計段階からのプライバシー」および「初期設定からのプライバシー保護」のアプローチを推奨しています。この取り組みにより、Grifols は関係者との信頼関係を構築し、個人データ漏えいによる評判上および経済的損失のリスクを軽減することで、持続可能な長期的成長および社会への責任に貢献します。

6.1.個人データ保護の原則

個人データを処理する Grifols の全従業員は、本方針に拘束されており、以下の原則に従う必要があります。

a. 合法的、公正かつ透明性のある方法で個人データを処理すること。 従業員は、Grifols が個人データを処理するにあたり、適切な法的根拠を有していることを常に確認しなければなりません。一般的に、法的根拠はデータ保護規制に定められており、これには以下が含まれます（ただし、これらに限定されません）：契約の履行に必要な個人データの処理（雇用契約など）、適用される法的義務の遵守（税務当局への個人データの提供など）、または、Grifols の正当な利益に基づく処理（ただし、データ主体の権利および自由を不当に侵害しない場合に限る。不正防止など）。適用されるデータ保護規制に従い、データ主体には、自身の個人データがどのように処理されるか、誰がその処理の責任を負うのか、またどこに提供される可能性があるのかなどについて、事前に通知されなければなりません。
b. 明示され、特定され、かつ正当な目的のためにのみ個人データを収集すること。 従業員は、合法的で明確に特定された目的のためにのみ個人データを収集することが許可されており、データ主体に開示した目的以外に個人データを使用することはできません。処理目的を変更する場

合は、事前にデータ主体に通知しなければならず、その変更には別の法的根拠が必要となる場合があり、データ主体の同意を取得する必要があることもあります。

c. 目的に照らして、適切で関連性があり、必要最小限の個人データのみを処理すること（データ最小化）。 従業員は、データ主体に開示された特定の目的のために必要な最小限の個人データのみを処理するものとします。目的達成に不要な個人データ、または特定の種類のデータについては、取得・処理してはなりません。

d. 正確かつ最新の個人データのみを処理すること。 従業員は、情報ライフサイクル（すなわち収集から廃棄まで）を通じて、個人データが正確かつ最新の状態であるよう、あらゆる合理的な措置を講じなければなりません。この点において、従業員は不正確な個人データを速やかに修正または削除するために、あらゆる合理的な努力を行わなければなりません。これには、関連する方針および手順に記載されているとおり、Grifols 内の複数の部門の関与および協力が必要となる場合があります。

e. 個人データは、処理目的の達成に必要な期間および法令に定められた期間のみ保管すること。 従業員は、個人データが処理される目的を達成するため、または法令により必要とされる場合に限り、Grifols のファイル（電子媒体および紙媒体の両方）に当該データを保管するものとします。保管が不要となった時点で、従業員は当該個人データを削除するためにあらゆる合理的な措置を講じなければなりません。これには、関連する方針および手順に記載されているとおり、Grifols 内の複数の部門の関与および協力が必要となる場合があります。

f. 安全な方法で個人データを処理すること。 Grifols は、個人データを保護し、その機密性、可用性を確保するとともに、必要に応じて規制に従い安全な方法で共有するために、組織的および技術的なセキュリティ対策を講じるものとします。Grifols の全従業員は、適用される技術的および組織的セキュリティ対策を遵守しなければなりません。これらの対策は、特に要配慮個人データを処理する際において重要です。

6.2.個人データに関するデータ主体の権利

データ保護規制は、個人に対して複数の権利を付与しており、その中には自己の個人データへのアクセス、誤った個人データの訂正、個人データの削除などが含まれます。これらの権利およびその行使方法については、Grifols が個人向けに提供しているプライバシー通知に明記されています。

適用される法令に基づき、個人データに関する個人の権利には、以下のようなものが含まれる場合があります。

- 情報への権利：個人データの処理に関して、簡潔で、透明性があり、理解しやすく、かつ容易にアクセス可能な情報を受け取る権利。一般的に、Grifols はプライバシー通知の中でこの情報を提供しており、そこには以下の内容が含まれます：管理者およびデータ保護責任者の連絡先、処理の目的およびその法的根拠（理由）、受領者のカテゴリー（存在する場合）、個人データの保存期間、以下に記載されるデータ保護に関する権利など。DPO および Grifol の法務顧問は、従業員と連携し、必要に応じてプライバシー通知を作成および／または改訂します。
- アクセス権：個人データが処理されているか否かについての確認を求める権利があり、処理されている場合には、Grifols が保有する個人データへのアクセスを請求することができます。
- 訂正権：不正確な個人データの修正を要求する権利。
- 削除権：個人データの削除を要求する権利。
- 処理の拒否権：特定の状況において、個人データの処理に対して異議を唱える権利。
- データポータビリティ権：Grifols に提供した個人データを、電子ファイルの形式で受け取る権利、およびこれを他の関係者に転送する権利。
- 処理の制限権：以下のいずれかの状況において、個人データの処理の制限を要求する権利：
  v. データ主体が個人データの正確性に異議を唱え、それが検証されている間。
  vi. 個人データの処理が違法であるが、データ主体がその削除に反対している場合。
  vii. Grifols は処理目的のために当該個人データをもはや必要としないが、データ主体が法的請求の立証、行使または防御のために必要としている場合。

viii. データ主体が公共の利益または正当な利益に基づく処理に異議を唱えており、Grifolsの正当な根拠がデータ主体の権利より優先するかどうかを確認中である場合。

- 同意の撤回権：既に提供した同意を撤回する権利。ただし、撤回前に同意に基づいて行われた処理の適法性には影響を与えません。

Grifols は、個人のデータ保護に関する権利の行使を円滑に管理するために、社内手順を定めています。データ主体の権利に関する要請を受け取ったGrifolsの従業員は、直ちに自組織内のデータ保護担当者または部門、または不在の場合は *Corporate Data Protection Office*（privacy@grifols.com）に連絡しなければなりません。

6.3.個人データの保存

個人データが、処理目的または適用される法的義務の遵守に必要でなくなった場合、従業員は、紙媒体を含むあらゆる物理的またはデジタル形式の個人データのすべてのコピーを破棄または削除するために、あらゆる合理的な措置を講じなければなりません。

この事項の詳細については、「Grifols データ保存方針（*"Records Retention Policy"* ID448）」を参照してください。

6.4.個人データのセキュリティおよびデータ漏えい

Grifols は、保有期間を通じて個人データを保護するための手順と技術を整備し、特に要配慮個人データに重点を置いて、個人データを安全に保つための合理的な技術的および組織的対策を講じています。さらに、これらの対策の有効性を確保するために、定期的な試験、評価および検証のプロセスを設けています。これにより、以下が確保されます。

a. 個人データの可用性：業務用情報システムおよび個人データが、必要な方法とタイミングで利用可能であること。Grifols は、偶発的または不正な喪失、破壊、損傷から保護するため、物理的または技術的インシデントが発生した場合に、速やかに個人データを復元できるよう、合理的な対策を講じています。

b. 個人データの機密性：個人データを保存するシステムおよびファイルには、正当に認可された者のみがアクセスでき、無断または偶発的、あるいは違法なアクセスや開示を防止します。

c. 個人データの完全性：個人データの正確性を維持し、偶発的または不正な改ざんを防止します。

全従業員は、IT セキュリティ方針を含む、該当するGrifolsの情報セキュリティ方針および手順に従って、個人データを処理しなければなりません。

個人データ漏えいは、可用性、機密性、完全性を損なうセキュリティインシデントの一種です。Grifols は、セキュリティインシデントおよび個人データ漏えいの報告のために、従業員が使用できる手順（DPO-SOP-000001_個人データインシデント手順書）を整備しています。これにより、Grifols はリスクおよびセキュリティ評価を実施し、必要に応じて監督機関や影響を受けた本人への通知義務を果たすことが可能となります。

6.5.個人データの移転およびサービス提供者

通常の業務の過程において、従業員が正当な業務上の理由、または法令により認められまたは義務付けられた理由に基づき、Grifols のグループ会社または第三者（複数の国にわたる可能性あり）にサービスを委託し、または個人データを移転する必要が生じる場合があります。

第三者機関に対して新たにサービスを委託する場合（既存のベンダーか新規かを問わず）、当該サービスが個人データの処理を伴うときは、データ主体の権利および自由に対するリスクと影響を評価するために、ベンダー評価を実施する必要があります。この評価の目的は、ベンダーが本方針および適用されるデータ保護規制に定められた原則および基準に従い、個人データを適切に保護・処理する能力を有していることを確認することです。

個人データの処理を含むすべての第三者または Grifols グループ会社とのサービス契約には、データ保護条項を含めるか、既に締結されたデータ保護契約への言及を含めなければなりません。

個人データの国際間移転は、適切な保護措置が講じられている場合にのみ許容されます。

Grifols は、国境を越えた個人データの移転およびサービス提供者の契約が、適用されるデータ保護規制に準拠していることを確認するための社内手順を整備しています。

6.6. トレーニングと意識向上

Grifols は、企業内における強固なプライバシー文化の醸成を目指しています。Grifols は、従業員が取り扱う個人データの処理内容に応じた適切なトレーニングを推進・提供し、意識向上と、個人データを適切に識別・取扱いできるよう教育しています。これにより、Grifols の社内基準・手順および適用されるプライバシー関連規制に準拠した業務運用を実現します。

6.7. デザインによるプライバシーとデフォルトによるプライバシー

従業員は、個人データのライフサイクル全体（すなわち収集から廃棄まで）にわたり、プライバシーおよびデータ保護の観点を考慮する必要があります。したがって、新しいプロジェクトの導入時などにおいては特に、業務活動の中にデータ保護の原則およびセキュリティ対策を組み込まなければなりません。また、技術的・組織的な適切なセキュリティ対策を講じ、必要最小限の個人データのみが処理されるようにすることが求められます。

7. 変更の理由

定義および関連文書の更新。

GRIFOLS

Global Privacy and Data Protection Policy

POLISH / POLSKI

INDEKS

GRIFOLS

1. CEL

Celem niniejszej Polityki ochrony prywatności i danych („polityki") jest wyjaśnienie obowiązujących zasad prywatności, które mają zastosowanie do spółek z Grupy Grifols ("Grifols") w celu ochrony i bezpieczeństwa danych osobowych oraz sposobu ich wdrażania.

Promowanie kultury szacunku dla danych osobowych wzmacnia relacje oparte na zaufaniu i przyczynia się do realizacji misji Grifols polegającej na poprawie zdrowia i samopoczucia ludzi na całym świecie.

2. ZAKRES

Niniejsza polityka obowiązuje wszystkie spółki grupy Grifols („Grifols") bez uszczerbku dla wszelkich przepisów dotyczących ochrony danych lub lokalnych przepisów mających zastosowanie do działalności biznesowej firmy Grifols, które mogą nakładać mniej lub bardziej surowe wymogi w zakresie ochrony prywatności i danych niż te obowiązujące na mocy niniejszej polityki. W związku z tym postanowienia niniejszej polityki muszą być interpretowane i egzekwowane zgodniez obowiązującymi przepisami prawa.

Niniejsza polityka dotyczy w szczególności wszystkich pracowników Grifols („pracowników"), którzy przetwarzają dane osobowe w ramach działań biznesowych prowadzonych przez Grifols. Dane osobowe to wszelkie informacje, które samodzielnie lub w połączeniu z innymi informacjami umożliwiają identyfikację danej osoby.

Niniejsza polityka nie dotyczy informacji ani danych, które nie stanowią danych osobowych.

3. POWIĄZANE DOKUMENTY

- *Kodeks postępowania firmy Grifols*
- *Polityka Grifols w zakresie praw człowieka*
- *Globalne warunki dla dostawcówInformation*
- *Security Policy (GHTI-CTRL-000237)*
- *Information Technology Usage Policy (CTRL-000110)*
- *Procedura dotycząca incydentów związanych z danymi osobowymi (DPO-SOP-000001)*
- *Polityka przechowywania dokumentacji ("Records Retention Policy" ID448)*

Więcej informacji na temat ochrony danych w Grifols można znaleźć w sekcji "Data Protection Office" w intranecie.

4. DEFINICJE

Do celów niniejszej polityki stosuje się poniższe terminy, którym przypisano następujące znaczenie:

TERMIN	DEFINICJA
Zgoda	Dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych.
Administrator	Osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który określa cele i sposoby przetwarzania danych osobowych.
Corporate Data Protection Office	Dział korporacyjny odpowiedzialny za wspieranie spółek grupy Grifols w kwestiach związanych z ochroną danych.

TERMIN	DEFINICJA
Przepisy dotyczące ochrony danych osobowych	Wszelkie przepisy, prawa, regulacje, ustawy, ustawy, uchwały, kodeksy, wytyczne lub postanowienia, w tym ich poprawki lub zmiany, dotyczące ochrony prywatności lub przetwarzania danych osobowych osób fizycznych w dowolnym kraju na świecie, mające zastosowanie do firmy Grifols, w tym bez ograniczeń RODO.
Inspektor ochrony danych (IOD)	Osoba, której zadaniem jest informowanie, doradzanie i monitorowanie właściwego przestrzegania wymogów dotyczących ochrony danych w Grifols, a także pełnienie funkcji punktu kontaktowego między Grifols, osobami, których dane dotyczą, a właściwym organem ochrony danych (IOD).
Osoba, której dane dotyczą / osoba fizyczna	Każda osoba, której dane osobowe są przetwarzane przez Grifols i którą można bezpośrednio lub pośrednio zidentyfikować na podstawie dostępnych danych osobowych (np. pracownicy, klienci, dawcy, pacjenci itp.).
Ogólne rozporządzenie o ochronie danych (RODO)	Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE.
Dane osobowe	Wszelkie informacje dotyczące osoby fizycznej, która jest lub może zostać zidentyfikowana: - bezpośrednio na podstawie tych informacji (np. imienia i nazwiska, numeru identyfikacyjnego, zdjęcia itp.); - pośrednio na podstawie tych informacji w połączeniu z innymi danymi (np. dokumentacja zdrowotna, ocena wyników, adres IP itd.).
Naruszenie ochrony danych osobowych	Każdy incydent związany z bezpieczeństwem, który skutkuje przypadkowym lub niezgodnym z prawem zniszczeniem, utratą, zmianą, przekazaniem lub uzyskaniem dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych przez Grifols lub przez stronę trzecią w imieniu Grifols. Wszystkie naruszenia ochrony danych osobowych są incydentami, ale nie wszystkie incydenty muszą być naruszeniami danych osobowych.
Oświadczenie o ochronie prywatności	Dokument skierowany do osób fizycznych zawierający informacje o przetwarzaniu danych osobowych.
Przetwarzanie	Wszelkie operacje wykonywane na danych osobowych w sposób zautomatyzowany lub niezautomatyzowany (np. zbieranie, utrwalanie, przechowywanie, hosting, modyfikowanie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, usuwanie itd.).
Szczególne kategorie danych osobowych / wrażliwe dane osobowe	Dane osobowe uznane za wrażliwe w świetle przepisów prawa i w związku z tym wymagające wyższego stopnia ochrony ze względu na prywatny charakter. Takie dane mogą być przetwarzane jedynie w ograniczonych okolicznościach. Oto kilka przykładów: - dane dotyczące rasy lub pochodzenia etnicznego; - poglądy polityczne; - wyznanie lub przekonania światopoglądowe; - przynależność do związków zawodowych; - dane genetyczne; - dane biometryczne przetwarzane wyłącznie w celu identyfikacji człowieka;

TERMIN	DEFINICJA
	- dane dotyczące zdrowia; - dane dotyczące życia seksualnego lub orientacji seksualnej; - dane dotyczące wyroków skazujących i naruszeń prawa; - Chronione informacje zdrowotne (*Protected Health Information* PHI).
Organ nadzorczy / organ ochrony danych	Niezależny organ publiczny odpowiedzialny za monitorowanie i egzekwowanie stosowania przepisów ustawowych i wykonawczych dotyczących ochrony danych. Do zadań organu ochrony danych należy również doradztwo w zakresie interpretacji obowiązujących przepisów prawa i, w stosownych przypadkach, nakładanie sankcji za naruszenia.
Strona trzecia	Osoby fizyczne lub prawne, organy publiczne, służby lub podmioty inne niż administrator danych, upoważnione do przetwarzania danych osobowych osób, których dane dotyczą, z którymi Grifols wchodzi w interakcje i które nie są firmą ani pracownikiem Grifols.

5. ROLE I OBOWIĄZKI

Zaangażowanie w ochronę prywatności i danych osobowych w Grifols rozpoczyna się od pracowników najwyższego szczebla – w szczególności zarządu. Stanowi ono jedną z zasad omówionych w Kodeksie postępowania firmy Grifols, dlatego stanowi integralną część naszej kultury organizacyjnej i działań biznesowych. W związku z tym dotyczy wszystkich pracowników firmy.

Pracownicy

Wszyscy pracownicy Grifols, którzy przetwarzają dane osobowe w ramach swojej działalności zawodowej, są zobowiązani do przestrzegania niniejszej polityki. Pracownicy powinni skontaktować się z osobą lub działem odpowiedzialnym za ochronę danych w swojej organizacji lub, w przypadku jej braku, z *Corporate Data Protection Office* (privacy@grifols.com), jeśli mają jakiekolwiek pytania dotyczące ich stosowania, a także w celu zgłoszenia potencjalnego naruszenia tych przepisów.

Corporate Data Protection Office

Corporate Data Protection Office jest odpowiedzialne za określenie globalnych ram ochrony prywatności Grifols oraz za nadzorowanie i koordynowanie zgodności z przepisami o ochronie danych.

Współpracuje ze wszystkimi działami i jednostkami biznesowymi Grifols w celu wzmocnienia poziomu wiedzy na temat ochrony danych wśród wszystkich pracowników, wspierania kultury prywatności i dostarczania rozwiązań, które umożliwiają operacyjną zgodność z przepisami o ochronie danych. Ostatecznym celem jest osiągnięcie poszanowania prawa ludzi do prywatności i ochrony ich danych osobowych.

Inspektor ochrony danych (IOD)

W przypadku spółek należących do grupy, w których powołano IOD, będzie on odpowiedzialny za następujące funkcje:

- Informowanie, doradzanie i monitorowanie zgodności z obowiązującymi przepisami o ochronie danych, w tym uświadamianie i szkolenie personelu zaangażowanego w operacje przetwarzania danych.
- Udzielanie porad w zakresie ocen skutków dla ochrony danych i monitorowanie ich wdrażania.
- Współpraca z organem nadzorczym we wszystkich sprawach związanych z przetwarzaniem danych osobowych.
- Pełnienie funkcji punktu kontaktowego dla organu i zainteresowanych stron

Inspektor ochrony danych wykonuje swoje funkcje z należytym uwzględnieniem ryzyka związanego z operacjami przetwarzania, biorąc pod uwagę charakter, zakres, kontekst i cele przetwarzania.

Dział Technologii Informacyjnych (IT)

Dział IT jest odpowiedzialny za zapewnienie stosowania technicznych i organizacyjnych środków bezpieczeństwa współmiernych do ryzyka związanego z przetwarzaniem danych osobowych, zgodnie ze wszystkimi zasadami określonymi w niniejszej polityce.

6. POLITYKA

Większość działań prowadzonych przez Grifols wiąże się z przetwarzaniem danych osobowych różnych interesariuszy, w tym m.in. pracowników, pacjentów, pracowników służby zdrowia, klientów, inwestorów, dostawców i darczyńców.

Grifols szanuje prawo do prywatności osób, które powierzają mu swoje dane osobowe i zobowiązuje się do przestrzegania obowiązujących przepisów o ochronie danych.

Zaangażowanie Grifols w przejrzystość, uczciwość i zasady wyszczególnione poniżej wykracza poza zwykłą zgodność z przepisami. Grifols promuje kulturę prywatności i ochrony danych osobowych poprzez podnoszenie świadomości pracowników na temat tego, czym one są i jak je chronić, a także poprzez przyjęcie podejścia opartego na ochronie prywatności w fazie projektowania i domyślnego. W ten sposób Grifols buduje relacje oparte na zaufaniu ze swoimi partnerami i zmniejsza ryzyko naruszenia bezpieczeństwa danych osobowych, co w konsekwencji powoduje szkody gospodarcze i wizerunkowe, przyczyniając się w ten sposób do długoterminowego, zrównoważonego rozwoju i zaangażowania na rzecz społeczeństwa.

6.1. Zasady ochrony danych osobowych

Wszyscy pracownicy Grifols, którzy przetwarzają dane osobowe, podlegają tej polityce i muszą przestrzegać następujących zasad:

a. Przetwarzanie danych osobowych w sposób zgodny z prawem, lojalny i przejrzysty. Pracownicy muszą zawsze upewnić się, że Grifols ma odpowiednie podstawy prawne do przetwarzania danych osobowych osób fizycznych. Ogólnie rzecz biorąc, podstawy prawne są określone w przepisach o ochronie danych osobowych i obejmują między innymi przetwarzanie danych osobowych w celu wykonania umowy (np. umowy o pracę), wypełnienia obowiązującego obowiązku prawnego (np. zgłaszania danych osobowych organom podatkowym) lub prawnie uzasadnionych interesów Grifols, o ile nie są one nadrzędne wobec praw i wolności osób, których dane dotyczą (np. zapobieganie oszustwom). Zgodnie z obowiązującymi przepisami o ochronie danych osobowych, osoby, których dane dotyczą, muszą być m.in. poinformowane o tym, w jaki sposób ich dane osobowe będą przetwarzane, kto będzie odpowiedzialny za przetwarzanie ich danych i komu mogą one zostać przekazane.

b. Gromadzenie danych osobowych wyłącznie do konkretnych, wyraźnych i prawnie uzasadnionych celów. Pracownicy mogą zbierać dane osobowe wyłącznie do konkretnych i wyraźnych celów, które są zgodne z prawem, i nie mogą wykorzystywać danych osobowych do celów innych niż przedstawione osobom, których dane dotyczą. Należy poinformować z wyprzedzeniem osoby, których dane dotyczą, o zmianach celów przetwarzania i w razie potrzeby przedstawić odmienne uzasadnienie prawne oraz uzyskać zgodę osoby, której dane dotyczą.

c. Przetwarzanie wyłącznie danych osobowych, które są adekwatne, stosowne i ograniczone do tego, co niezbędne do celów, dla których są przetwarzane. (minimalizacja danych). Pracownicy będą przetwarzać tylko minimalną ilość danych osobowych wymaganych do określonego celu, o którym została poinformowana osoba, której dane dotyczą. Jeśli takie dane nie są wymagane, nie wolno ich żądać ani w żaden sposób przetwarzać.

d. Przetwarzanie tylko danych osobowych, które są prawidłowe i aktualizowane. Pracownicy są zobowiązani do podjęcia wszelkich uzasadnionych kroków w celu zagwarantowania, że przetwarzane dane osobowe są prawidłowe i aktualizowane przez cały cykl życia informacji (tj. od momentu zgromadzenia danych do ich zniszczenia). W związku z tym pracownicy są zobowiązani podejmować wszelkie uzasadnione starania w celu niezwłocznego sprostowania lub usunięcia nieprawidłowych danych osobowych. Może to wymagać zaangażowania i współpracy kilku działów firmy Grifols zgodnie z obowiązującymi zasadami i procedurami.

e. Przechowywać dane osobowe tylko tak długo, jak jest to konieczne do spełnienia celów przetwarzania i obowiązujących zobowiązań prawnych. Pracownicy mogą przechowywać dane osobowe w zbiorach firmy Grifols (zarówno w formacie elektronicznym, jak i papierowym) wyłącznie przez okres, w którym są one potrzebne do realizacji celów przetwarzania, lub jeśli jest to wymagane na mocy prawa. Pracownicy są zobowiązani do podjęcia wszelkich uzasadnionych działań służących usunięciu danych osobowych, gdy ich przechowywanie nie jest już wymagane. Może to wymagać zaangażowania i współpracy kilku działów firmy Grifols zgodnie z obowiązującymi zasadami i procedurami.

f. Przetwarzanie danych osobowych w bezpieczny sposób. Grifols przyjmie techniczne i organizacyjne środki bezpieczeństwa w celu ochrony danych osobowych, zapewnienia ich poufności, integralności i dostępności oraz, w stosownych przypadkach, udostępnienia ich w sposób bezpieczny i zgodny z przepisami. Wszyscy pracownicy Grifols muszą przestrzegać obowiązujących technicznych i organizacyjnych środków bezpieczeństwa, które są szczególnie ważne przy przetwarzaniu szczególnych kategorii danych osobowych.

6.2. Prawa osób fizycznych w odniesieniu do ich danych osobowych

Na mocy przepisów dotyczących ochrony danych osobom fizycznym przysługują rozmaite prawa, w tym między innymi prawo dostępu do swoich danych osobowych, prawo do sprostowania nieprawidłowych danych osobowych lub ich usunięcia. Firma Grifols przekazuje osobom fizycznym oświadczenia o ochronie prywatności, w których dokładnie omówiono te prawa i sposoby ich wykonywania.

W zależności od obowiązujących przepisów, prawa osób, których dane dotyczą, w odniesieniu do ich danych osobowych mogą obejmować:

- Prawo do informacji: prawo do otrzymania zwięzłych, przejrzystych, zrozumiałych i łatwo dostępnych informacji na temat przetwarzania danych osobowych. Zasadniczo firma Grifols podaje informacje na ten temat w oświadczeniach o ochronie prywatności, które zawierają między innymi dane kontaktowe administratora i inspektora ochrony danych oraz omówienie celów i podstawy prawnej przetwarzania (powodów przetwarzania), kategorii odbiorców (jeśli dotyczy), okresu przechowywania danych osobowych oraz praw związanych z ochroną danych omówionych poniżej. W razie potrzeby IOD oraz radcy prawni Grifols będą rozwijać i/lub zmieniać oświadczenia o ochronie prywatności.
- Prawo dostępu: prawo do żądania potwierdzenia, czy dane osobowe są przetwarzane, a jeśli tak, do uzyskania dostępu do danych osobowych zawartych w zbiorach Grifols.
- Prawo do sprostowania: prawo do żądania poprawienia nieprawidłowych danych osobowych.
- Prawo do usunięcia danych: prawo do żądania usunięcia danych osobowych.
- Prawo do sprzeciwu: prawo do żądania zaprzestania przetwarzania danych osobowych w określonych okolicznościach.
- Prawo do przenoszenia: prawo do żądania otrzymania pliku elektronicznego zawierającego dane osobowe przekazane firmie Grifols, a także prawo do przesłania ich innym stronom.
- Prawo do ograniczenia przetwarzania: prawo do żądania ograniczenia przetwarzania danych osobowych w przypadku, gdy:
  i. trwa weryfikacja danych osobowych po zakwestionowaniu ich prawidłowości;
  ii. przetwarzanie danych osobowych jest niezgodne z prawem, a osoba, której dane dotyczą, sprzeciwia się ich usunięciu;
  iii. firma Grifols nie potrzebuje już danych osobowych do celów przetwarzania, ale przetwarzanie jest wymagane do ustalenia, dochodzenia lub obrony roszczeń;
  iv. osoba, której dane dotyczą, wniosła sprzeciw wobec przetwarzania na podstawie prawnie uzasadnionego interesu lub interesu publicznego, przez czas niezbędny do sprawdzenia, czy prawnie uzasadnione podstawy Grifols są nadrzędne wobec podstaw osoby, której dane dotyczą.
- Prawo do wycofania zgody: prawo do wycofania udzielonej zgody bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej wycofaniem.

Firma Grifols ustanawia wewnętrzne procedury, które ułatwiają osobom fizycznym korzystanie z praw w zakresie ochrony danych i umożliwiają zarządzanie żądaniami związanymi z takimi prawami. Każdy pracownik Grifols, który otrzyma od osoby, której dane dotyczą, wniosek o skorzystanie z przysługujących jej praw, musi niezwłocznie skontaktować się z osobą lub działem odpowiedzialnym za ochronę danych w swojej organizacji lub, w przypadku jego braku, z *Corporate Data Protection Office* (privacy@grifols.com).

6.3. Zatrzymywanie danych osobowych

Gdy dane osobowe nie są już potrzebne do celów, w których są przetwarzane, ani do wywiązania się ze stosownych obowiązków prawnych, pracownicy są zobowiązani podjąć wszelkie uzasadnione działania służące zniszczeniu lub usunięciu wszystkich kopii danych osobowych zarówno w formie drukowanej, jak i na innym fizycznym lub elektronicznym nośniku pamięci.

Więcej informacji na ten temat można znaleźć w Polityce przechowywania danych firmy Grifols (*"Records Retention Policy"* ID448).

6.4. Bezpieczeństwo danych i naruszenia ochrony danych

Firma Grifols wdraża procedury i rozwiązania techniczne służące zabezpieczaniu danych osobowych przez cały okres ich przechowywania. W tym celu firma Grifols wdraża uzasadnione środki techniczne i organizacyjne służące zapewnieniu bezpieczeństwa danych osobowych i dokłada dodatkowych starań w przypadku szczególnych kategorii danych osobowych. Firma Grifols opracowuje również proces służący regularnemu testowaniu, ocenianiu i analizowaniu skuteczności tych środków w celu spełnienia następujących warunków:

a. Dostępność danych osobowych: w celu zagwarantowania, że firmowe systemy informatyczne oraz dane osobowe mogą być wykorzystywane w wymagany sposób, gdy są potrzebne. Grifols stosuje uzasadnione środki zapewniające ochronę przed przypadkową lub nieautoryzowaną utratą, zniszczeniem lub uszkodzeniem i umożliwiające szybkie przywrócenie danych osobowych w razie incydentu fizycznego lub technicznego.

b. Poufność danych osobowych: w celu zabezpieczenia danych osobowych i zagwarantowania, że dostęp do systemu jest przyznany jedynie upoważnionym osobom, aby zapobiec nieupoważnionemu, przypadkowemu lub niezgodnemu z prawem dostępowi do danych osobowych lub ich ujawnienia.

c. Integralność danych osobowych**:** w celu utrzymania prawidłowości danych osobowych i zabezpieczenia ich przed przypadkową lub nieuczciwą modyfikacją.

Wszyscy pracownicy przetwarzający dane osobowe są zobowiązani do przestrzegania obowiązujących zasad i procedur firmy Grifols związanych z bezpieczeństwem informacji, w tym między innymi Polityki bezpieczeństwa informatycznego.

Naruszenia danych osobowych to rodzaj incydentu bezpieczeństwa, który zagraża dostępności, poufności lub integralności danych osobowych. Grifols opracował procedury (DPO-SOP-000001_ Procedura dotycząca incydentów związanych z danymi osobowymi) umożliwiające pracownikom wewnętrzne zgłaszanie incydentów i naruszeń bezpieczeństwa danych osobowych, tak aby Grifols był w stanie przeprowadzić odpowiednią ocenę ryzyka i bezpieczeństwa oraz w stosownych przypadkach wywiązać się z obowiązków powiadomienia organu ochrony danych i osób, których dane dotyczą, których to dotyczy.

6.5. Przekazywanie danych osobowych oraz usługodawcy

W normalnym toku działalności firmy może zajść konieczność zlecenia usługi i/lub przekazania danych osobowych spółce grupy Grifols lub stronom trzecim w wielu krajach z uzasadnionych powodów biznesowych bądź z innych przyczyn dopuszczonych lub wymaganych na mocy prawa.

W przypadku zawarcia umowy na nową usługę od strony trzeciej (niezależnie od tego, czy jest to istniejący, czy nowy dostawca), która wiąże się z przetwarzaniem danych osobowych, należy przeprowadzić ocenę dostawcy w celu oceny ryzyka i wpływu takiego przetwarzania na prawa i wolności osób, których dane dotyczą. Celem takiej oceny jest potwierdzenie, że dostawca posiada zdolność do ochrony i przetwarzania danych osobowych zgodnie z zasadami i standardami określonymi w niniejszej polityce oraz w przepisach obowiązujących przepisów o ochronie danych.

Wszystkie umowy o świadczenie usług z osobami trzecimi lub spółkami z grupy Grifols, które wiążą się z przetwarzaniem danych osobowych, muszą zawierać klauzule o ochronie danych lub odniesienie do umowy o ochronie danych, która została już sformalizowana.

Transgraniczne przekazywanie danych osobowych będzie dopuszczalne tylko wtedy, gdy zapewnione zostaną odpowiednie zabezpieczenia.

Grifols ustanawia wewnętrzne procedury mające na celu weryfikację, czy przekazywanie danych osobowych między krajami i zawieranie umów z usługodawcami jest zgodne z obowiązującymi przepisami o ochronie danych.

6.6. Szkolenia i zwiększanie świadomości

Grifols dąży do tworzenia silnej kultury ochrony prywatności w firmie. W tym celu promuje i zapewnia swoim pracownikom odpowiednie szkolenia, proporcjonalne do przetwarzanych przez nich danych osobowych, które mają na celu zwiększenie świadomości i edukację w zakresie identyfikowania i przetwarzania danych osobowych w sposób zgodny z zasadami i procedurami Grifols oraz obowiązującymi przepisami o ochronie danych.

6.7. Uwzględnianie ochrony danych w fazie projektowania oraz domyślna ochrona danych

Pracownicy powinni uwzględniać kwestie ochrony prywatności i danych przez cały cykl życia danych osobowych (tj. od momentu ich zebrania do zniszczenia). W związku z tym są zobowiązani stosować zasady ochrony danych i odpowiednie środki bezpieczeństwa we wszystkich działaniach biznesowych na rzecz firmy Grifols, w szczególności podczas realizacji nowych. Ponadto wdrożone zostaną odpowiednie techniczne i organizacyjne środki bezpieczeństwa w celu zapewnienia, że domyślnie przetwarzane są tylko te dane osobowe, które są absolutnie niezbędne do każdego celu.

7. UZASADNIENIE ZMIAN

Aktualizacja definicji i powiązanych dokumentów.

GRIFOLS

Global Privacy and Data Protection Policy

PORTUGUESE / PORTUGUÊS

ÍNDICE

GRIFOLS

1. OBJETIVO

O objetivo da presente Política de Privacidade e de Proteção de Dados (a "política") consiste em explicar quais os princípios relevantes de privacidade que se aplicam às empresas do Grupo Grifols ("Grifols") para a proteção e segurança de dados pessoais e a forma como esses princípios são implementados.

Promover uma cultura de respeito pelos dados pessoais fortalece as relações de confiança e contribui para a missão da Grifols de melhorar a saúde e o bem-estar das pessoas em todo o mundo.

2. ÂMBITO

A presente política aplica-se a todas as empresas do grupo Grifols ("Grifols") sem prejuízo de quaisquer regulamentos de proteção de dados ou da legislação local aplicável às atividades comerciais da Grifols, que possam resultar em disposições de privacidade e de proteção de dados menos ou mais rigorosas do que as reguladas na presente política. Desta forma, as disposições estabelecidas na presente política deverão ser interpretadas e aplicadas de acordo com a legislação aplicável.

Especificamente, a presente política aplica-se a todos os colaboradores da Grifols (os “colaboradores”) que tratam dados pessoais como parte das atividades empresariais realizadas pela Grifols. Dados pessoais são quaisquer informações que de forma direta ou em combinação com outras informações permitem a identificação de um indivíduo.

A presente política não se aplica a informações ou dados que não sejam dados pessoais.

3. DOCUMENTOS RELACIONADOS

- *Código de Conduta da Grifols*
- *Política de Direitos Humanos da Grifols*
- *Termos e condições globais para fornecedores*
- *Information Security Policy (GHTI-CTRL-000237)*
- *Information Technology Usage Policy (CTRL-000110)*
- *Procedimento relativo a incidentes de dados pessoais (DPO-SOP-000001)*
- *Política de Conservação de Registos (“Records Retention Policy” ID448)*

Pode encontrar mais informações sobre proteção de dados na Grifols na secção "Data Protection Office" da intranet.

4. DEFINIÇÕES

Para efeitos da presente política, os termos indicados abaixo terão o seguinte significado:

TERMO	DEFINIÇÃO
Consentimento	Qualquer manifestação de vontade livre, específica, informada e inequívoca de uma pessoa física que aceite, por meio de uma declaração ou de uma ação afirmativa clara, o tratamento dos dados pessoais que lhe dizem respeito.
Responsável pelo Tratamento	Pessoa física ou jurídica, autoridade pública, agência ou outro organismo que determina os fins e os meios de tratamento de dados pessoais.
Corporate Data Protection Office	Departamento corporativo responsável por apoiar as empresas do grupo Grifols em matéria de proteção de dados.

TERMO	DEFINIÇÃO
Regulamentos de Proteção de Dados	Qualquer lei, norma, resolução, código, diretriz, ato ou disposição, incluindo as respetivas alterações ou substituições relacionadas com a privacidade ou o tratamento de dados pessoais de indivíduos em qualquer país do mundo, aplicável à Grifols, incluindo, entre outros, o RGPD e a LGPD (Brasil).
Encarregado da Proteção de Dados (EPD)	Pessoa encarregada de informar, assessorar e supervisionar o correto cumprimento de questões relacionadas com a proteção de dados na Grifols e que também serve como ponto de contato entre a Grifols, os titulares dos dados e a Autoridade Nacional de Proteção de Dados competente (ANPD).
Titular dos Dados/Indivíduo	Qualquer pessoa cujos dados pessoais estão a ser tratados pela Grifols e que pode ser identificada, direta ou indiretamente com base nos dados pessoais disponíveis (por exemplo: colaboradores, clientes, dadores, doentes, etc.).
Regulamento Geral sobre a Proteção de Dados (RGPD) / (LGPD)	Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, e que revoga a diretiva 95/46/CE. A Lei Geral de Proteção de Dados (LGPD), Lei nº 13.709/2018, é uma lei brasileira que estabelece diretrizes para o tratamento de dados pessoais, buscando proteger a privacidade e os direitos fundamentais das pessoas. A LGPD define como dados pessoais informações que permitam identificar uma pessoa, direta ou indiretamente.
Dados Pessoais/Informações, Pessoais	Qualquer informação relativa a um indivíduo que pode ser identificado ou identificável: - Diretamente, por referência a essas informações (por exemplo: nome, número de identificação pessoal, fotografia, etc.) - Indiretamente, a partir dessas informações em combinação com outros dados (por exemplo: registos clínicos, avaliação de desempenho, endereço IP, etc.).
Incidente/Violação de Dados Pessoais	Qualquer incidente de segurança que resulte na destruição, perda, alteração, comunicação ou acesso acidental ou ilegal a dados pessoais transmitidos, armazenados ou processados de qualquer forma pela Grifols ou por terceiros em nome da Grifols. Todas as violações de dados pessoais são incidentes, mas nem todos os incidentes são necessariamente violações de dados pessoais.
Aviso de Privacidade	Documento dirigido às pessoas físicas, que contém informações sobre o tratamento de dados pessoais.
Tratamento	Qualquer operação automatizada ou não que envolva dados pessoais (por exemplo: coleta, , registro, armazenamento, processamento , alteração, consulta, uso, publicação, transmissão, eliminação, etc.).
Categorias Especiais de Dados Pessoais/Dados, Pessoais Sensíveis	Dados pessoais considerados sensíveis por lei e que são, por conseguinte, merecedores de um nível mais elevado de proteção, devido à sua natureza privada, e que só podem ser tratados em circunstâncias limitadas. Seguem alguns exemplos:

TERMO	DEFINIÇÃO
	- Origens raciais ou étnicas - Opiniões políticas - Crenças religiosas ou filosóficas - Filiação em sindicatos - Dados genéticos - Dados biométricos tratados exclusivamente para identificar uma pessoa física - Dados relacionados com a saúde - Dados relativos à vida sexual ou orientação sexual - Condenações e infrações criminais - Informações de saúde protegidas (*Protected Health Information, PHI*)
Autoridade de Controle/Autoridade Nacional de Proteção de Dados (ANPD)	Autoridade pública independente responsável pela monitorização e cumprimento da aplicação das leis e regulamentos de proteção de dados a nível nacional. A ANPD também fornece orientações sobre a interpretação da legislação e, conforme o caso, impõe penalizações por descumprimento.
Terceiros	Pessoas físicas ou jurídicas, autoridades públicas, serviços ou organismos que não sejam responsáveis pelo tratamento, autorizados a tratar os dados pessoais dos titulares dos dados, com os quais a Grifols interage e que não sejam uma empresa ou colaborador da Grifols.

5. FUNÇÕES E RESPONSABILIDADES

A privacidade e a proteção de dados na Grifols começa no mais alto nível da empresa, sendo lideradas pela Direção Executiva. Tal como qualquer um dos princípios do Código de Conduta da Grifols, elas fazem parte integrante da nossa cultura e atividades empresariais e dizem respeito a todos dentro da empresa.

Colaboradores

Todos os colaboradores da Grifols cuja atividade consista em processar dados pessoais devem seguir a presente política. Caso existam quaisquer dúvidas sobre a aplicação da presente política e para comunicar qualquer possível violação identificada, os colaboradores deverão entrar em contacto com a pessoa ou departamento responsável pela proteção de dados em sua organização ou, na sua falta, com *Corporate Data Protection Office* (privacy@grifols.com).

Corporate Data Protection Office

Corporate Data Protection Office é responsável por definir a estrutura de privacidade global da Grifols e por supervisionar e coordenar a conformidade com os regulamentos de proteção de dados.

Colabora com todos os departamentos e unidades de negócio da Grifols para reforçar o nível de conhecimento em proteção de dados entre todos os colaboradores, fomentando uma cultura de privacidade e fornecendo soluções que permitam o cumprimento operacional das normas de proteção de dados. O objetivo final é alcançar o respeito pelo direito das pessoas à privacidade e à proteção de seus dados pessoais.

Encarregado da Proteção de Dados (EPD)

Para as empresas do grupo nas quais um EPD foi nomeado, ele será responsável pelas seguintes funções:

- Informar, aconselhar e monitorar o cumprimento dos regulamentos de proteção de dados aplicáveis, incluindo conscientização e treinamento do pessoal envolvido nas operações de processamento de dados.

- Prestar aconselhamento sobre avaliações de impacto sobre a proteção de dados e acompanhar a sua implementação.
- Cooperar com a autoridade de controle em todas as questões relacionadas com o tratamento de dados pessoais.
- Atuar como ponto de contato para a autoridade e partes interessadas.

O EPD deve desempenhar as suas funções tendo em consideração os riscos associados às operações de tratamento, considerando a natureza, o âmbito, o contexto e as finalidades do tratamento.

Departamento de Tecnologia da Informação TI

O departamento de TI é responsável por garantir que as medidas de segurança técnicas e organizacionais estejam em vigor de acordo com o risco associado ao processamento de dados pessoais, e conforme todos os princípios estabelecidos nesta política.

6. POLÍTICA

A maioria das atividades realizadas pela Grifols envolve o tratamento de dados pessoais de várias partes interessadas, incluindo colaboradores, pacientes, profissionais de saúde, clientes, investidores, fornecedores e doadores, entre outros.

A Grifols respeita os direitos de privacidade dos indivíduos que lhe confiam os seus dados pessoais e compromete-se a cumprir os regulamentos de proteção de dados aplicáveis.

O compromisso da Grifols com a transparência, integridade e os princípios detalhados abaixo vão além da mera conformidade regulatória. A Grifols promove uma cultura de privacidade e proteção de dados pessoais, conscientizando os colaboradores sobre o que são e como protegê-los, bem como adotando uma abordagem de privacidade desde o princípio e de fato. Desta forma, a Grifols gera relações de confiança com os seus parceiros e mitiga o risco de violações da segurança dos dados pessoais, com os consequentes danos econômicos e reputacionais, contribuindo assim para o crescimento sustentável da Grifols a longo prazo e para o seu compromisso com a sociedade.

6.1. Princípios de Proteção de Dados Pessoais

Todos os colaboradores da Grifols que tratam dados pessoais estão sujeitos a esta política e devem seguir os seguintes princípios:

a. Tratar os dados pessoais de forma legal, justa e transparente. Os colaboradores devem garantir sempre que a Grifols tenha justificativa legal adequada para processar os dados pessoais de pessoas físicas. Em geral, as bases legais são estabelecidas nos regulamentos de proteção de dados e incluem, mas não se limitam a, o processamento de dados pessoais para a execução de um contrato (por exemplo, um contrato de trabalho), o cumprimento de uma obrigação legal aplicável (por exemplo, relatar dados pessoais às administrações públicas) ou os interesses legítimos da Grifols, desde que não se sobreponham aos direitos e liberdades dos titulares dos dados (por exemplo, prevenção de fraudes). De acordo com o disposto na regulamentação aplicável em matéria de proteção de dados, os titulares dos dados devem ser previamente informados sobre a forma como os seus dados pessoais serão tratados, quem será o responsável pelo tratamento dos seus dados e a quem poderão ser comunicados, entre outros aspectos.

b. Recolher dados pessoais apenas para fins especificados, explícitos e legítimos. Os colaboradores podem recolher dados pessoais apenas para o(s) fim(ns) específico(s), explícito(s) e legal(ais) e não podem utilizar os dados pessoais para outros fins que não os comunicados previamente aos titulares dos dados. As alterações na finalidade a que se destina o tratamento deverá ser comunicadas antecipadamente ao titular dos dados e devem estar embasadas em uma justificativa legal, podendo ser necessário obter o consentimento do titular dos dados.

c. Tratar apenas dados pessoais que sejam adequados, relevantes e no limite do necessário no âmbito dos fins a que se destinam (minimização de dados). Os colaboradores deverão processar

apenas os dados pessoais mínimos necessários para o fim específico que foi comunicado ao titular dos dados. Se esses dados não forem necessários, não devem ser solicitados ou processados de forma alguma.

d. Tratar apenas dados pessoais que sejam exatos e atualizados. Os colaboradores deverão adotar todas as medidas razoáveis para garantir que os dados pessoais que tratam são exatos e estão atualizados ao longo de todo o ciclo de vida da informação (ou seja, desde a coleta até a destruição). Dessa forma, os colaboradores envidarão todos os esforços razoáveis para retificar ou apagar dados pessoais inexatos de imediato. Isto pode exigir o envolvimento e colaboração de vários departamentos dentro da Grifols, conforme descrito nas políticas e procedimentos pertinentes.

e. Conservar os dados pessoais apenas durante o período de tempo necessário para cumprir as finalidades do tratamento e as obrigações legais aplicáveis. Os colaboradores conservarão os dados pessoais nos arquivos da Grifols (tanto em formato eletrónico como em papel) apenas enquanto for necessário para cumprir os fins para os quais os dados pessoais devam ser tratados ou quando legalmente necessário. Os colaboradores deverão adotar todas as medidas razoáveis para apagar os dados pessoais quando deixar de ser necessária a conservação dos mesmos. Isto pode exigir o envolvimento e colaboração de vários departamentos dentro da Grifols, conforme descrito nas políticas e procedimentos pertinentes.

f. Tratar os dados pessoais de forma segura. A Grifols adotará medidas de segurança técnicas e organizacionais para proteger os dados pessoais, garantir sua confidencialidade, integridade e disponibilidade e, se aplicável, compartilhá-los de forma segura e em conformidade com os regulamentos. Todos os colaboradores da Grifols devem observar as medidas de segurança técnicas e organizacionais aplicáveis, que são especialmente importantes no tratamento de categorias especiais de dados pessoais.

6.2. Direitos das pessoas físicas sobre os seus dados pessoais

Os regulamentos de proteção de dados conferem às pessoas físicas vários direitos, incluindo, entre outros, o acesso aos respectivos dados pessoais, a correção de quaisquer dados pessoais incorretos ou a eliminação dos seus dados pessoais. Estes direitos, bem como a forma como os direitos devem ser exercidos, estão estabelecidos de forma clara nos avisos de privacidade da Grifols que estão à disposição dos interessados.

Dependendo dos regulamentos aplicáveis, os direitos dos titulares dos dados em relação aos seus dados pessoais podem incluir o seguinte:

- Informação: o direito de receber informações concisas, transparentes, inteligíveis e de fácil acesso sobre o tratamento de dados pessoais. Em geral, a Grifols fornece estas informações em avisos de privacidade que incluem as informações de contato do responsável pelo tratamento de dados e do encarregado da proteção de dados, os fins e a base legal (o porquê) para o tratamento, as categorias de destinatários (se aplicável), o período de conservação dos dados pessoais e os direitos de proteção de dados mencionados abaixo, entre outros. O EPD e os consultores jurídicos da Grifols, em colaboração com os colaboradores, deverão elaborar e/ou revisar os avisos de privacidade, conforme necessário.
- Acesso: o direito de solicitar confirmação sobre se e como os dados pessoais estão, ou não, sendo tratados e, em caso afirmativo, de obter acesso aos dados pessoais incluídos nos arquivos da Grifols.
- Retificação: o direito de solicitar a alteração de dados pessoais inexatos.
- Eliminação: o direito de solicitar que os dados pessoais sejam eliminados.
- Oposição: o direito de solicitar que os dados pessoais não sejam tratados em circunstâncias específicas.
- Portabilidade: o direito de solicitar que lhe sejam enviados, em formato eletrónico, os dados pessoais fornecidos à Grifols, bem como o direito de transmití-los a terceiros.
- Limitação do tratamento: o direito de solicitar a limitação da forma como os dados pessoais são tratados quando:

i. estiver sendo verificada a exatidão dos dados pessoais após terem sido contestados;
ii. o tratamento dos dados pessoais for ilícito e o titular dos dados se opuser à sua eliminação;
iii. a Grifols já não necessitar dos dados pessoais para os fins do tratamento, mas os dados forem solicitados pelo indivíduo para a postulação, o exercício ou a defesa em ações judiciais ou reclamações, e
iv. o titular dos dados se opôs ao tratamento com base no interesse legítimo ou interesse público, durante o tempo necessário para verificar se os motivos legítimos da Grifols prevalecem sobre os do interessado.

- Revogação do consentimento: o direito de retirar o consentimento fornecido sem afetar a legalidade do tratamento com base no consentimento fornecido antes da sua retirada.

A Grifols estabelece procedimentos internos para facilitar e gerir o exercício dos direitos de proteção de dados das pessoas físicas. Qualquer colaborador da Grifols que receba uma solicitação de um interessado que prtene exercer seus deverá contatar imediatamente a pessoa ou departamento responsável pela proteção de dados em sua organização ou, na falta destes, com o *Corporate Data Protection Office* (privacy@grifols.com).

6.3. Conservação de Dados Pessoais

Quando os dados pessoais já não forem necessários para a finalidade para a qual estão sendo tratados ou para o cumprimentodas obrigações legais aplicáveis, os colaboradores deverão adotar todas as medidas razoáveis para destruir ou apagar todas as cópias de dados pessoais, seja em papel ou em qualquer outro meio de armazenamento físico ou eletrônico.

Para mais informações sobre esta questão, consulte a Política de Conservação de Dados da Grifols (*"Records Retention Policy" ID448*).

6.4. Segurança dos dados pessoais e violações de segurança

A Grifols aplica procedimentos e tecnologia para proteger os dados pessoais enquanto os conservar, adotando medidas técnicas e organizacionais razoáveis para manter a segurança dos dados pessoais, com especial atenção às categorias especiais de dados pessoais. A Grifols também estabelece um processo periódico para comprovar, verificar, avaliar e valorar a eficácia dessas medidas, a fim de garantir a:

a. Disponibilidade dos dados pessoais: que os sistemas de informação da empresa e os dados pessoais estejam acessíveis na forma e no tempo necessários. A Grifols adota medidas razoáveis para proteger os dados pessoais contra a perda, a destruição ou o dano acidental ou não autorizado, para poder restaurar prontamente os dados pessoais em caso de incidente físico ou técnico.

b. Confidencialidade dos dados pessoais: que apenas pessoas devidamente autorizadas acessem os sistemas e arquivos que armazenam dados pessoais, impedindo o acesso ou comunicações não autorizadas, acidentais ou ilícitas de dados pessoais.

c. Integridade dos dados pessoais**:** para manter a exatidão dos dados pessoais contra quaisquer alterações acidentais ou fraudulentas.

Todos os colaboradores deverão cumprir as políticas e procedimentos de segurança de informação da Grifols aplicáveis no tratamento de dados pessoais, incluindo, mas não se limitando a "*Information Security Policy*„ de TI.

As violações de dados pessoais são um tipo de incidente de segurança que põem em risco a disponibilidade, confidencialidade ou integridade dos dados pessoais. A Grifols elaborou procedimentos (DPO-SOP-000001_ *Procedimento relativo a incidentes de dados pessoais*) para que os colaboradores notifiquem internamente incidentes e violações de segurança de dados pessoais, para que a Grifols esteja em condições de realizar a avaliação de risco e segurança correspondente e cumprir, quando

apropriado, com as obrigações de notificar a autoridade de proteção de dados e os titulares dos dados afetados.

6.5. Transferências de Dados Pessoais e Prestadores de Serviços

Durante o desempenho das suas atividades normais, os colaboradores podem necessitar contratar um serviço e/ou de transferir dados pessoais às empresas do grupo Grifols ou a terceiros emdiferentes países por razões comerciais legítimas ou por exigência legal.

Quando um novo serviço é contratado de um terceiro (seja um fornecedor existente ou novo) que envolve o processamento de dados pessoais, uma avaliação do terceiro deve ser realizada, para avaliar o risco e o impacto de tal processamento nos direitos e liberdades dos titulares dos dados. O objetivo de tal avaliação é confirmar que o fornecedor tem a capacidade de proteger e processar dados pessoais de acordo com os princípios e padrões estabelecidos nesta política e nas disposições dos regulamentos de proteção de dados aplicáveis.

Todos os contratos de prestação de serviços com terceiros ou com empresas do grupo Grifols que envolvam o tratamento de dados pessoais deverão incluir cláusulas de proteção de dados ou fazer referência a um contrato de proteção de dados já formalizado.

As transferências de dados pessoais entre países só serão aceitáveis se estiverem implementadas as garantias adequadas.

A Grifols estabelece procedimentos internos para verificar que as transferências de dados pessoais entre países e a contratação de prestadores de serviços cumprem os regulamentos em proteção de dados.

6.6. Formação e Conscientização

A Grifols procura promover uma forte cultura de privacidade dentro da empresa. A Grifols promove e fornece formação adequada aos seus colaboradores, proporcional ao tratamento de dados pessoais que realizam, com o objetivo de conscientizar e educar sobre como identificar e tratar os dados pessoais em conformidade com as normas e procedimentos da Grifols e com os regulamentos de proteção de dados aplicáveis.

6.7. Privacidade desde a Conceção e Privacidade por Defeito

Os colaboradores deverão ter em conta questões de privacidade e proteção de dados durante todo o ciclo de vida dos dados pessoais (ou seja, desde a recolha até à destruição) e, portanto, deverão integrar os princípios de proteção de dados e as medidas de segurança nas suas atividades profissionais executadas na Grifols, em particular ao implementar um novo projeto. Adicionalmente, serão implementadas medidas de segurança técnicas e organizativas adequadas para garantir que, por defeito, apenas sejam tratados os dados pessoais estritamente necessários para cada finalidade.

7. RAZÕES PARA A MUDANÇA

Atualização de definições e documentos relacionados.

GRIFOLS

Global Privacy and Data Protection Policy

SPANISH / ESPAÑOL

ÍNDICE

GRIFOLS

1. OBJETIVO

El objetivo de esta Política de Privacidad y Protección de Datos (la «política») es explicar los principios relevantes en materia de privacidad que aplican a las empresas del Grupo Grifols («Grifols») para la protección y la seguridad de los datos personales y cómo se implementan estos principios.

Fomentar una cultura de respeto hacia los datos personales fortalece las relaciones de confianza y contribuye a la misión de Grifols de mejorar la salud y el bienestar de las personas en todo el mundo.

2. ÁMBITO DE APLICACIÓN

Esta política aplica a todas las empresas del Grupo Grifols, sin perjuicio de las normas de protección de datos o leyes locales aplicables a sus actividades comerciales, que pueden establecer disposiciones de privacidad y protección de datos más o menos estrictas que las reguladas en esta política. Las disposiciones de esta política deben interpretarse y aplicarse en concordancia con la legislación vigente.

En concreto, esta política aplica a todos los empleados de Grifols (los «empleados») que tratan datos personales en el marco de las actividades empresariales que realiza Grifols. Se entiende por «datos personales» toda información que directamente o en combinación con otra, permita la identificación de una persona física.

Esta política no se aplica a información o datos que no sean datos personales.

3. DOCUMENTOS RELACIONADOS

- *Código de conducta de Grifols*
- *Política de derechos humanos de Grifols*
- *Términos y condiciones globales para proveedores*
- *Política de seguridad de la Información (GHTI-CTRL-000237)*
- *Política de normas de uso de sistemas informáticos (CTRL-000110)*
- *Procedimiento relativo a incidentes de datos personales (DPO-SOP-000001)*
- *Política de conservación de documentación ("Records Retention Policy" ID448)*

Puedes encontrar más información sobre la protección de datos en Grifols en la sección "Data Protection Office" de la intranet.

4. DEFINICIONES

A los efectos de esta política, los términos que figuran a continuación tendrán el siguiente significado:

TÉRMINO	DEFINICIÓN
Consentimiento	Toda manifestación de voluntad libre, específica, informada e inequívoca por la que una persona acepta, ya sea mediante una declaración o una acción afirmativa clara, el tratamiento de datos personales que le conciernen.
Responsable del tratamiento	La persona física o jurídica, autoridad pública, agencia u otro organismo que determine los fines y medios del tratamiento de datos personales.
Corporate Data Protection Office	Departamento corporativo encargado de apoyar a las empresas del grupo Grifols en asuntos de protección de datos.

TÉRMINO	DEFINICIÓN
Normativas sobre protección de datos/privacidad	Toda ley, norma, estatuto, acto, resolución, código, guía o disposición, incluidas sus modificaciones o sustituciones, en relación con la privacidad o el tratamiento de datos personales de individuos en cualquier país del mundo, a los que esté sujeto Grifols, incluido, sin carácter limitativo, el RGPD.
Delegado de Protección de Datos (DPD)	Persona designada para informar, asesorar y supervisar el correcto cumplimiento de los asuntos relativos a la protección de datos en Grifols y que actúa, asimismo, como punto de contacto entre Grifols, los interesados y la Autoridad de Protección de Datos (APD) competente.
Interesado / Persona física	Toda persona física cuyos datos personales trata Grifols y cuya identidad puede determinarse, directa o indirectamente, mediante los datos personales disponibles (p.ej. empleados, clientes, donantes, pacientes, etc.).
Reglamento General de Protección de Datos (RGPD)	Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE.
Datos Personales / Información Personal	Toda información sobre una persona física identificada o identificable: - Directamente mediante esa información (p.ej., nombre, número de identificación, foto, etc.) - Indirectamente mediante esa información en combinación con otros datos (p.ej, historial médico, evaluación del desempeño, dirección IP, etc.).
Incidente/Brecha de Datos Personales	Todo incidente de seguridad que dé lugar a la destrucción, pérdida, alteración, comunicación o acceso accidentales o ilícitos a datos personales transmitidos, conservados o tratados de otro modo por Grifols o por un tercero por cuenta de Grifols. Todas las brechas de seguridad de datos personales son incidentes, pero no todos los incidentes son necesariamente brechas de seguridad de datos personales.
Aviso de privacidad	Documento dirigido a personas físicas que contiene información sobre el tratamiento de datos personales.
Tratamiento	Cualquier operación, ya sea por procedimientos automatizados o no, con datos personales (p.ej. recogida, registro, conservación, alojamiento, modificación, consulta, utilización, comunicación por transmisión, supresión, etc.).
Categorías especiales de datos personales / Datos personales sensibles	Datos personales considerados sensibles por ley y, por tanto, merecedores de un mayor grado de protección por su naturaleza privada y que solo pueden tratarse en circunstancias limitadas. A continuación, figuran algunos ejemplos: - Origen étnico o racial - Opiniones políticas - Convicciones religiosas o filosóficas - Afiliación sindical - Datos genéticos - Datos biométricos dirigidos únicamente a identificar a una persona física - Datos relativos a la salud - Datos relativos a la vida sexual o la orientación sexual - Condenas e infracciones penales

TÉRMINO	DEFINICIÓN
	- Información de salud protegida (*Protected Health Information (PHI)*
Autoridad de Control / Autoridad de Protección de Datos (APD)	Autoridad pública independiente responsable de la supervisión y la aplicación de las leyes y normas de protección de datos. La APD también ofrece orientación sobre la interpretación de la legislación y, en su caso, impone sanciones por incumplimiento.
Tercero	Personas físicas o jurídicas, autoridades públicas, servicios u organismos distintos del responsable del tratamiento, autorizados para tratar los datos personales de los interesados, con los que Grifols interactúa y que no son una empresa o un empleado de Grifols.

5. FUNCIONES Y RESPONSABILIDADES

La protección de la privacidad y de los datos en Grifols comienza en el nivel más alto de la empresa, promovida desde la Dirección Ejecutiva. Como uno de los principios del Código de conducta de Grifols, forma parte integral de nuestra cultura y actividad empresarial, y concierne a todos los miembros de la empresa.

Empleados

Todos los empleados de Grifols que traten datos personales en el marco de su actividad profesional tienen la obligación de cumplir con esta política. Los empleados deben ponerse en contacto con la persona o departamento encargado de la protección de datos en su organización o, en su defecto, con la *Corporate Data Protection Office* (privacy@grifols.com) si tienen alguna duda sobre la aplicación de la misma, así como para notificar cualquier potencial infracción de la misma.

Corporate Data Protection Office

La *Corporate Data Protection Office* es responsable de definir el marco global de privacidad de Grifols, y de supervisar y coordinar el cumplimiento de las normativas de protección de datos.

Colabora con todos los departamentos y unidades de negocio de Grifols para reforzar el nivel de conocimiento en materia de protección de datos entre todos los empleados, fomentando una cultura de la privacidad y proporcionando soluciones que permitan cumplir de manera operativa con las regulaciones de protección de datos. El objetivo final es lograr el respeto al derecho de las personas a la privacidad y protección de sus datos personales.

Delegado de Protección de Datos (DPD)

Para las compañías del grupo en las que se haya designado un DPD, este será responsable de las siguientes funciones:

- Informar, asesorar y supervisar el cumplimiento de las normativas de protección de datos aplicables, incluyendo la concienciación y la formación del personal involucrado en las operaciones de tratamiento de datos.
- Ofrecer asesoramiento acerca de las evaluaciones de impacto relativas a la protección de datos y supervisar su ejecución.
- Cooperar con la autoridad de control en todas las cuestiones relativas al tratamiento de datos personales.
- Actuar como punto de contacto de la autoridad y de los interesados

El DPD llevará a cabo sus funciones prestando la debida atención a los riesgos asociados a las operaciones de tratamiento, teniendo en cuenta la naturaleza, el alcance, el contexto y fines del tratamiento.

Departamento de Tecnología de la Información (IT)

El departamento de IT es responsable de garantizar que se apliquen medidas de seguridad técnicas y organizativas proporcionales al riesgo asociado al tratamiento de datos personales, de conformidad con todos los principios recogidos en esta política.

6. POLÍTICA

La mayoría de las actividades que realiza Grifols conllevan el tratamiento de datos personales de diversos grupos de interés, incluyendo empleados, pacientes, profesionales sanitarios, clientes, inversores, proveedores y donantes, entre otros.

Grifols respeta los derechos de privacidad de las personas que le confían sus datos personales y se compromete a cumplir con las normativas de protección de datos aplicables.

El compromiso de Grifols con la transparencia, integridad y los principios que se detallan a continuación va más allá del mero cumplimiento normativo. Grifols fomenta una cultura de privacidad y protección de los datos personales mediante la concienciación de los empleados sobre qué son y cómo protegerlos, así como mediante la adopción de un enfoque de privacidad desde el diseño y por defecto. De esta manera, Grifols genera relaciones de confianza con sus interlocutores y mitiga el riesgo de que se produzcan brechas de la seguridad de los datos personales, con los consecuentes daños económicos y reputacionales, contribuyendo así al crecimiento sostenible de Grifols a largo plazo y a su compromiso con la sociedad.

6.1. Principios de protección de datos personales

Todos los empleados de Grifols que traten datos personales están sujetos a esta política y deben seguir los principios que figuran a continuación:

a. Tratar los datos personales de manera lícita, leal y transparente. Los empleados deben asegurarse en todo momento de que Grifols tenga una justificación legal adecuada para tratar los datos personales de personas físicas. Por lo general, las bases jurídicas se establecen en las normativas de protección de datos e incluyen, entre otras, el tratamiento de datos personales para la ejecución de un contrato (p.ej. un contrato de trabajo), el cumplimiento de una obligación legal aplicable (p.ej. comunicar datos personales a las administraciones tributarias) o intereses legítimos de Grifols, siempre y cuando estos no prevalezcan sobre los derechos y libertades de los interesados (p.ej. prevención del fraude). Con arreglo a lo dispuesto en las normativas aplicables de protección de datos, se deberá informar previamente a los interesados sobre cómo se tratarán sus datos personales, quién será el responsable del tratamiento de sus datos y a quién podrán comunicarse, entre otros aspectos.

b. Recoger datos personales únicamente para fines específicos, explícitos y legítimos. Los empleados están autorizados a recoger datos personales solo para fines específicos y explícitos que sean lícitos, y no podrán utilizarlos para fines distintos de aquellos comunicados a los interesados. Todo cambio en la finalidad del tratamiento debe comunicarse previamente al interesado y debería ir respaldado por una base jurídica, pudiendo ser necesario obtener el consentimiento del interesado.

c. Tratar únicamente datos personales que sean adecuados, pertinentes y limitados a lo necesario en relación con los fines (minimización de datos). Los empleados solo tratarán los datos personales mínimos requeridos para el fin específico que se haya comunicado al interesado. Si dichos datos no fueran necesarios, no deben solicitarse ni tratarse de ningún modo.

d. Tratar únicamente datos personales exactos y actualizados. Los empleados deberán adoptar todas las medidas razonables para que los datos personales que tratan sean exactos y estén actualizados durante la totalidad del ciclo de vida de la información (es decir, desde la recogida hasta la destrucción). En este sentido, los empleados harán todo lo razonablemente posible para rectificar o suprimir sin dilación los datos personales inexactos, para lo que puede ser necesaria

la participación y la colaboración de varios departamentos de Grifols, como se describe en las políticas y en los procedimientos pertinentes.

e. Conservar los datos personales únicamente durante el tiempo necesario para cumplir con los fines del tratamiento y las obligaciones legales aplicables. Los empleados conservarán los datos personales en los archivos de Grifols (tanto en formato electrónico como en papel) únicamente mientras sea necesario para cumplir los fines para los que se tratan los datos personales o cuando sea legalmente necesario. Los empleados deberán adoptar todas las medidas razonables para suprimir los datos personales cuando dejen de ser necesarios, para lo que puede ser precisa la participación y colaboración de varios departamentos de Grifols, como se describe en las políticas y en los procedimientos pertinentes.

f. Tratar los datos personales de forma segura. Grifols adoptará medidas de seguridad técnicas y organizativas para proteger los datos personales, asegurar su confidencialidad, integridad y disponibilidad y si aplica, compartirlos de manera segura y de conformidad con la normativa. Todos los empleados de Grifols deben observar las medidas de seguridad técnicas y organizativas que sean aplicables, las cuales son especialmente importantes cuando se tratan categorías especiales de datos personales.

6.2. Derechos de las personas físicas sobre sus datos personales

Las normativas de protección de datos confieren a las personas físicas varios derechos, incluyendo, entre otros, el derecho a acceder a sus datos personales, a la rectificación de cualquier dato personal erróneo o a la supresión de sus datos personales. Estos derechos y la manera de ejercerlos se establecen claramente en los avisos de privacidad que Grifols pone a disposición de los interesados.

En función de la normativa aplicable, los derechos de los interesados en relación con sus datos personales, pueden incluir los siguientes:

- Información: derecho a recibir información concisa, transparente, inteligible y de fácil acceso sobre el tratamiento de datos personales. Por lo general, Grifols facilita esta información en los avisos de privacidad, en los que se incluyen los datos de contacto del responsable del tratamiento y del DPD, los fines y la base jurídica (por qué) del tratamiento, las categorías de destinatarios (si aplica), el plazo de conservación de los datos personales y los derechos de protección de datos mencionados a continuación, entre otros. El DPD y los asesores jurídicos de Grifols, con la colaboración de los empleados, elaborarán y/o revisarán los avisos de privacidad según sea necesario.
- Acceso: derecho a solicitar confirmación sobre si se están tratando o no datos personales y, en su caso, a obtener acceso a los datos personales incluidos en los ficheros de Grifols.
- Rectificación: derecho a solicitar la modificación de datos personales inexactos.
- Supresión: derecho a solicitar la eliminación de los datos personales.
- Oposición: derecho a solicitar que los datos personales no se traten en circunstancias específicas.
- Portabilidad: derecho a solicitar la entrega, en un archivo electrónico, de los datos personales facilitados a Grifols, y derecho a transmitirlos a terceros.
- Limitación del tratamiento: derecho a solicitar la limitación del tratamiento de los datos personales cuando:
  i. se esté verificando la exactitud de los datos personales tras haber sido impugnados;
  ii. el tratamiento de datos personales sea ilícito y el interesado se oponga a su supresión;
  iii. Grifols ya no necesite los datos personales para los fines del tratamiento, pero estos sean necesarios para la formulación, el ejercicio o la defensa de reclamaciones, y
  iv. el interesado se haya opuesto al tratamiento basado en el interés legítimo o en interés público, durante el tiempo necesario para verificar si los motivos legítimos de Grifols prevalecen sobre los del interesado.
- Revocación del consentimiento: derecho a revocar el consentimiento prestado, sin que ello afecte a la licitud del tratamiento basado en el consentimiento previo a su retirada.

Grifols establece procedimientos internos para facilitar y gestionar el ejercicio de los derechos de protección de datos de las personas físicas. Todo empleado de Grifols que reciba la solicitud de un interesado para ejercer sus derechos deberá ponerse en contacto inmediatamente con la persona o departamento encargado de la protección de datos en su organización o en su defecto con la *Corporate Data Protection Office* (privacy@grifols.com).

6.3. Conservación de datos personales

Cuando los datos personales ya no sean necesarios para el fin para el que se tratan o para cumplir con las obligaciones legales aplicables, los empleados adoptarán todas las medidas razonables para destruir o eliminar todas las copias de dichos datos personales, ya sea en papel o en cualquier otro soporte de almacenamiento físico o electrónico.

Para más información, consulte la Política de Conservación de Datos de Grifols (*"Records Retention Policy" ID448*).

6.4. Seguridad de los datos personales y brechas de seguridad

Grifols aplica procedimientos y tecnología para proteger los datos personales durante el tiempo que los conserva adoptando medidas técnicas y organizativas razonables a fin de mantener la seguridad de los datos personales, con especial atención a las categorías especiales de datos personales. Grifols establece asimismo un proceso periódico de comprobación, evaluación y valoración de la eficacia de estas medidas, con el fin de asegurar la:

a. Disponibilidad de los datos personales: que los sistemas de información de la empresa y los datos personales sean accesibles en la forma y el tiempo requeridos. Grifols adopta medidas razonables para proteger los datos personales frente a la pérdida, la destrucción o los daños accidentales o no autorizados, y para poder restaurar rápidamente los datos personales en caso de incidente físico o técnico.

b. Confidencialidad de los datos personales: que solo las personas debidamente autorizadas acceden a los sistemas y archivos que albergan datos personales, evitando el acceso o las comunicaciones no autorizadas, accidentales o ilícitas de los datos personales.

c. Integridad de los datos personales**:** mantener la exactitud de los datos personales frente a cualquier alteración accidental o fraudulenta.

Todos los empleados deberán cumplir las políticas y los procedimientos de seguridad de la información de Grifols aplicables al tratamiento de datos personales, incluida, sin carácter limitativo, la Política de seguridad de la Información.

Las brechas de seguridad de datos personales son un tipo de incidente de seguridad que pone en peligro la disponibilidad, la confidencialidad o la integridad de los mismos. Grifols ha diseñado procedimientos (DPO-SOP-000001_ *Procedimiento relativo a incidentes de datos personales*) para que los empleados notifiquen internamente los incidentes y brechas de seguridad de los datos personales, de manera que Grifols esté en condiciones de realizar la correspondiente evaluación de riesgos y seguridad y cumplir, en su caso, con las obligaciones de notificación a la autoridad de protección de datos y a los interesados afectados.

6.5. Transferencias de datos personales y proveedores de servicios

Durante el curso normal de sus actividades, los empleados pueden tener la necesidad de contratar un servicio o transferir datos personales a empresas del grupo Grifols o a terceros en diferentes países por motivos de negocio legítimos o según lo exija la ley.

Cuando se contrata un nuevo servicio de un tercero (ya se trate de un proveedor existente o nuevo) que conlleve el tratamiento de datos personales, se deberá realizar una evaluación del proveedor, para valorar el riesgo y el impacto de dicho tratamiento en los derechos y libertades de los interesados. El

objetivo de dicha evaluación es confirmar que el proveedor tiene la capacidad de proteger y tratar los datos personales de acuerdo con los principios y normas establecidos en esta política y en las disposiciones de la normativa aplicable de protección de datos.

Todos los contratos de servicios con terceros o con empresas del grupo Grifols que conlleven el tratamiento de datos personales deben incluir cláusulas de protección de datos o una referencia a un contrato de protección de datos ya formalizado.

Las transferencias transfronterizas de datos personales solo serán aceptables si existen garantías adecuadas.

Grifols establece procedimientos internos para verificar que las transferencias de datos personales entre países y la contratación de proveedores de servicios cumplen la normativa en materia de protección de datos aplicable.

6.6. Formación y concienciación

Grifols aspira a fomentar una sólida cultura de privacidad en la empresa. Para ello, promueve e imparte formación adecuada a sus empleados, proporcional al tratamiento de datos personales que realizan y que tiene como objetivo concienciar y educar sobre cómo identificar y tratar los datos personales de modo que se cumplan las normas y procedimientos de Grifols y las normativas de protección de datos aplicables.

6.7. Privacidad desde el diseño y privacidad por defecto

Los empleados deben tener en cuenta las cuestiones relativas a la privacidad y la protección de datos durante la totalidad del ciclo de vida de los datos personales (es decir, desde la recogida hasta la destrucción) y, por tanto, deben integrar los principios de protección de datos y las medidas de seguridad en todas las actividades profesionales que llevan a cabo en Grifols pero, en especial, a la hora de ejecutar un nuevo proyecto. Además, se aplicarán las medidas de seguridad técnicas y organizativas apropiadas para garantizar que, por defecto, solo se traten los datos personales estrictamente necesarios para cada finalidad.

7. MOTIVO DEL CAMBIO

Actualización de definiciones y documentos relacionados .

GRIFOLS

Global Privacy and Data Protection Policy

THAI / ไทย

ดัชนี

GRIFOLS

1. วัตถุประสงค์

วัตถุประสงค์ของนโยบายความเป็นส่วนตัวและการคุ้มครองข้อมูลฉบับนี้ ("นโยบาย")
คือการอธิบายหลักการด้านความเป็นส่วนตัวที่เกี่ยวข้องซึ่งบังคับใช้กับบริษัทในเครือทั้งหมดของกลุ่ม Grifols ("Grifols")
สำหรับการคุ้มครองและความปลอดภัยของข้อมูลส่วนบุคคล ตลอดจนวิธีการดำเนินการตามหลักการดังกล่าว

การส่งเสริมวัฒนธรรมแห่งความเคารพต่อข้อมูลส่วนบุคคลช่วยเสริมสร้างความสัมพันธ์ที่ตั้งอยู่บนความไว้วางใจ และส่งเสริมภารกิจของ Grifols ในการพัฒนาสุขภาพและความเป็นอยู่ที่ดีของผู้คนทั่วโลก

2. ขอบเขต

นโยบายฉบับนี้บังคับใช้กับบริษัทในเครือทั้งหมดของกลุ่ม Grifols
โดยไม่กระทบต่อกฎระเบียบด้านการคุ้มครองข้อมูลหรือกฎหมายท้องถิ่นที่บังคับใช้กับกิจกรรมทางธุรกิจ
ซึ่งอาจกำหนดข้อกำหนดด้านความเป็นส่วนตัวและการคุ้มครองข้อมูลที่เข้มงวดมากหรือน้อยกว่าที่กำหนดไว้ในนโยบายฉบับนี้ ดังนั้น
ข้อกำหนดของนโยบายฉบับนี้จึงควรได้รับการตีความและดำเนินการให้สอดคล้องกับกฎหมายที่ใช้บังคับ

โดยเฉพาะอย่างยิ่ง นโยบายฉบับนี้บังคับใช้กับพนักงานทุกคนของ Grifols ("พนักงาน") ที่มีหน้าที่ประมวลผลข้อมูลส่วนบุคคล
อันเป็นส่วนหนึ่งของกิจกรรมทางธุรกิจที่ดำเนินการโดย Grifols ข้อมูลส่วนบุคคลคือข้อมูลใด ๆ ที่สามารถระบุตัวตนของบุคคลได้
ไม่ว่าจะโดยทางตรงหรือโดยการใช้ร่วมกับข้อมูลอื่น

นโยบายฉบับนี้ไม่บังคับใช้กับข้อมูลหรือสารสนเทศที่ไม่เป็นข้อมูลส่วนบุคคล

3. เอกสารที่เกี่ยวข้อง

- *หลักจรรยาบรรณในการดำเนินธุรกิจของ Grifols*
- *นโยบายด้านสิทธิมนุษยชนของ Grifols*
- *ข้อกำหนดและเงื่อนไขสากลสำหรับผู้จัดจำหน่าย*
- *นโยบายความมั่นคงปลอดภัยของข้อมูล - "Information Security Policy" (GHTI-CTRL-000237)*
- *นโยบายการใช้เทคโนโลยีสารสนเทศ - "Information Technology Usage Policy" (CTRL-000110)*
- *ระเบียบปฏิบัติกรณีเกิดเหตุการณ์เกี่ยวกับข้อมูลส่วนบุคคล (DPO-SOP-000001)*
- *นโยบายการเก็บรักษาเอกสารและข้อมูล - "Records Retention Policy" (ID448)*

คุณสามารถค้นหาข้อมูลเพิ่มเติมเกี่ยวกับความเป็นส่วนตัวใน *Grifols* ได้ที่ส่วน *Data Protection Office* บนระบบอินทราเน็ต

4. คำนิยาม

เพื่อวัตถุประสงค์ของนโยบายฉบับนี้ คำศัพท์ที่ระบุไว้ด้านล่างจะมีความหมายดังต่อไปนี้:

คำศัพท์	คำนิยาม
ความยินยอม	การแสดงเจตนาอย่างอิสระ เฉพาะเจาะจง โดยได้รับข้อมูลครบถ้วน และไม่คลุมเครือของบุคคลใดบุคคลหนึ่ง ซึ่งแสดงออกผ่านคำพูดหรือการกระทำที่ชัดเจน เพื่อแสดงความยินยอมให้มีการประมวลผลข้อมูลส่วนบุคคลที่เกี่ยวข้องกับตนเอง
ผู้ควบคุมข้อมูล	บุคคลธรรมดาหรือนิติบุคคล หน่วยงานของรัฐ องค์กร หรือหน่วยงานอื่นใดที่เป็นผู้กำหนดวัตถุประสงค์และวิธีการในการประมวลผลข้อมูลส่วนบุคคล
สำนักงานคุ้มครองข้อมูลส่วนบุคคลขององค์กร - *„Corporate Data Protection Office“*	หน่วยงานส่วนกลางขององค์กรที่มีหน้าที่ให้การสนับสนุนบริษัทในเครือของกลุ่ม Grifols ในเรื่องที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล
กฎหมายและระเบียบข้อบังคับว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล/ความเป็นส่วนตัว	กฎหมาย กฎ ระเบียบ พระราชบัญญัติ มติ ประมวลกฎหมาย แนวทางปฏิบัติ หรือข้อกำหนดใด ๆ รวมถึงการแก้ไขหรือการแทนที่ในอนาคต ซึ่งเกี่ยวข้องกับความเป็นส่วนตัวหรือการประมวลผลข้อมูลส่วนบุคคลของบุคคลในประเทศ

GRIFOLS

คำศัพท์	คำนิยาม
	ใด ๆ ทั่วโลก และใช้บังคับกับ Grifols รวมถึงแต่ไม่จำกัดเพียงกฎระเบียบว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป (GDPR)
เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล – *Data Protection Officer* (DPO)	บุคคลธรรมดาหรือนิติบุคคลที่ได้รับการแต่งตั้งให้ทำหน้าที่ให้ข้อมูล ให้คำแนะนำ และตรวจสอบการปฏิบัติตามข้อกำหนดด้านการคุ้มครองข้อมูลภายใน Grifols อย่างถูกต้อง พร้อมทั้งทำหน้าที่เป็นจุดติดต่อระหว่าง Grifols กับเจ้าของข้อมูลส่วนบุคคลและหน่วยงานผู้มีอำนาจด้านการคุ้มครองข้อมูล (DPA)
เจ้าของข้อมูลส่วนบุคคล / บุคคลธรรมดา	บุคคลใดก็ตามที่ข้อมูลส่วนบุคคลของตนกำลังถูกประมวลผลโดย Grifols และสามารถระบุตัวตนได้ ไม่ว่าจะโดยทางตรงหรือทางอ้อม จากข้อมูลส่วนบุคคลที่มีอยู่ (เช่น พนักงาน ลูกค้า ผู้บริจาคโลหิต ผู้ป่วย เป็นต้น)
ระเบียบทั่วไปว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล (GDPR)	ระเบียบ (EU) 2016/679 ของรัฐสภายุโรปและของคณะมนตรี ลงวันที่ 27 เมษายน 2016 ว่าด้วยการคุ้มครองบุคคลธรรมดาในเรื่องการประมวลผลข้อมูลส่วนบุคคลและการเคลื่อนย้ายข้อมูลดังกล่าวอย่างเสรี และเป็นการยกเลิกคำสั่ง 95/46/EC
ข้อมูลส่วนบุคคล / สารสนเทศส่วนบุคคล	ข้อมูลใด ๆ ที่เกี่ยวข้องกับบุคคลธรรมดาที่สามารถระบุตัวตนได้ หรืออาจสามารถระบุตัวตนได้ โดยทางตรงจากข้อมูลนั้นเอง (เช่น ชื่อ เลขประจำตัว รูปถ่าย เป็นต้น) โดยทางอ้อมจากข้อมูลนั้นเมื่อใช้ร่วมกับข้อมูลอื่น (เช่น เวชระเบียน ผลการประเมินผลการปฏิบัติงาน ที่อยู่ IP เป็นต้น)
การละเมิด/เหตุการณ์เกี่ยวกับข้อมูลส่วนบุคคล	เหตุการณ์ด้านความมั่นคงปลอดภัยที่นำไปสู่การทำลาย สูญหาย เปลี่ยนแปลง เปิดเผย หรือเข้าถึงข้อมูลส่วนบุคคลโดยไม่ได้ตั้งใจหรือโดยมิชอบด้วยกฎหมาย ซึ่งข้อมูลนั้นถูกส่ง เก็บรักษา หรือประมวลผลโดย Grifols หรือโดยบุคคลภายนอกที่ดำเนินการแทน Grifols การละเมิดข้อมูลส่วนบุคคลทุกกรณีถือเป็นเหตุการณ์ที่เกี่ยวข้องกับข้อมูลส่วนบุคคล แต่ไม่ใช่ทุกเหตุการณ์ที่จะถือเป็นการละเมิดข้อมูลส่วนบุคคลเสมอไป
ประกาศความเป็นส่วนตัว	เอกสารที่จัดทำขึ้นสำหรับบุคคลทั่วไป ซึ่งมีข้อมูลเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคล
การประมวลผล	การดำเนินการใด ๆ ไม่ว่าจะโดยอัตโนมัติหรือไม่ก็ตาม ที่เกี่ยวข้องกับข้อมูลส่วนบุคคล (เช่น การเก็บรวบรวม การบันทึก การจัดเก็บ การโฮสต์ การแก้ไข การเข้าถึง การใช้ การเผยแพร่ การส่งต่อ การลบ เป็นต้น)
ข้อมูลส่วนบุคคลประเภทพิเศษ / ข้อมูลอ่อนไหว	ข้อมูลส่วนบุคคลที่กฎหมายถือว่าเป็นข้อมูลที่มีความอ่อนไหวและจำเป็นต้องได้รับการคุ้มครองในระดับสูงกว่า เนื่องจากมีลักษณะเฉพาะด้านความเป็นส่วนตัว และสามารถประมวลผลได้เฉพาะในสถานการณ์ที่จำกัดเท่านั้น ตัวอย่างของข้อมูลประเภทนี้ ได้แก่: เชื้อชาติหรือชาติพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อทางศาสนาหรือปรัชญา การเป็นสมาชิกสหภาพแรงงาน ข้อมูลทางพันธุกรรม ข้อมูลชีวภาพที่ถูกประมวลผลเพื่อใช้ในการระบุบุคคลเท่านั้น ข้อมูลที่เกี่ยวข้องกับสุขภาพ ข้อมูลเกี่ยวกับชีวิตทางเพศหรือรสนิยมทางเพศ การตัดสินลงโทษทางอาญาและความผิดทางอาญา

คำศัพท์	คำนิยาม
	ข้อมูลสุขภาพที่ได้รับการคุ้มครอง (Protected Health Information - PHI)
หน่วยงานกำกับดูแล / หน่วยงานคุ้มครองข้อมูลส่วนบุคคล (DPA)	หน่วยงานสาธารณะที่เป็นอิสระ ซึ่งมีหน้าที่ในการกำกับดูแลและบังคับใช้กฎหมายและระเบียบข้อบังคับด้านการคุ้มครองข้อมูลส่วนบุคคล หน่วยงานคุ้มครองข้อมูลส่วนบุคคล (DPA) ยังมีหน้าที่ให้คำแนะนำเกี่ยวกับการตีความกฎหมาย และในกรณีที่จำเป็น สามารถกำหนดบทลงโทษในกรณีที่มีการไม่ปฏิบัติตามกฎหมายดังกล่าวได้ด้วย
บุคคลภายนอก	บุคคลธรรมดาหรือนิติบุคคล หน่วยงานของรัฐ องค์กร หรือหน่วยงานอื่นที่ไม่ใช่ผู้ประมวลผลข้อมูลหรือไม่ได้เป็นบริษัทในเครือของ Grifols หรือพนักงานของ Grifols แต่ได้รับอนุญาตให้ประมวลผลข้อมูลส่วนบุคคลของเจ้าของข้อมูล และมีความเกี่ยวข้องหรือมีปฏิสัมพันธ์กับ Grifols

5. บทบาทและความรับผิดชอบ

การดำเนินงานด้านความเป็นส่วนตัวและการคุ้มครองข้อมูลที่ Grifols เริ่มต้นจากระดับสูงสุด
โดยมีฝ่ายผู้บริหารระดับสูงเป็นผู้นำในการขับเคลื่อน ในฐานะที่เป็นหนึ่งในหลักการของจรรยาบรรณในการดำเนินธุรกิจของ Grifols
เรื่องนี้จึงถือเป็นส่วนสำคัญของวัฒนธรรมองค์กรและกิจกรรมทางธุรกิจของเรา และเป็นเรื่องที่เกี่ยวข้องกับทุกคนภายในบริษัท

พนักงาน

พนักงานทุกคนของ Grifols ที่มีหน้าที่เกี่ยวข้องกับการจัดการข้อมูลส่วนบุคคลในการปฏิบัติงาน
มีหน้าที่ในการปฏิบัติตามนโยบายฉบับนี้อย่างเคร่งครัด
พนักงานควรติดต่อบุคคลหรือหน่วยงานที่รับผิดชอบด้านความเป็นส่วนตัวในองค์กรของตน หรือ Corporate Data Protection Office (privacy@grifols.com) หากมีข้อสงสัยเกี่ยวกับการนำแนวทางในนโยบายนี้ไปปฏิบัติ
หรือเพื่อรายงานกรณีที่อาจเป็นการละเมิดนโยบายที่ตรวจพบ

Corporate Data Protection Office - สำนักงานคุ้มครองข้อมูลส่วนบุคคลส่วนกลางขององค์กร

สำนักงานคุ้มครองข้อมูลส่วนบุคคลส่วนกลางขององค์กรมีหน้าที่กำหนดกรอบแนวทางด้านความเป็นส่วนตัวในระดับสากลของ Grifols
รวมถึงกำกับดูแลและประสานงานให้มีการปฏิบัติตามกฎหมายและระเบียบข้อบังคับด้านการคุ้มครองข้อมูลส่วนบุคคลอย่างเหมาะสม

สำนักงานฯ ทำงานร่วมกับทุกแผนกและหน่วยธุรกิจของ Grifols
เพื่อเสริมสร้างความตระหนักรู้ด้านการคุ้มครองข้อมูลส่วนบุคคลในหมู่พนักงานทุกคน ส่งเสริมวัฒนธรรมด้านความเป็นส่วนตัว
และจัดหาแนวทางแก้ไขที่เอื้อให้สามารถดำเนินงานให้สอดคล้องกับข้อบังคับด้านความเป็นส่วนตัวได้อย่างมีประสิทธิภาพ
เป้าหมายสูงสุดของสำนักงานคือการส่งเสริมและบรรลุความเคารพต่อสิทธิความเป็นส่วนตัวและการคุ้มครองข้อมูลส่วนบุคคลของทุกคน

เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)

สำหรับบริษัทในเครือที่มีการแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) เจ้าหน้าที่ผู้นี้จะมีหน้าที่รับผิดชอบในด้านต่าง ๆ ดังต่อไปนี้:

- ให้ข้อมูล คำแนะนำ และตรวจสอบการปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลที่เกี่ยวข้อง
  รวมถึงการสร้างความตระหนักรู้และให้การฝึกอบรมแก่บุคลากรที่เกี่ยวข้องกับการดำเนินงานด้านการประมวลผลข้อมูล
- ให้คำแนะนำเกี่ยวกับการประเมินผลกระทบด้านการคุ้มครองข้อมูล และติดตามการดำเนินการตามที่ได้ประเมินไว้
- ให้ความร่วมมือกับหน่วยงานกำกับดูแลในทุกเรื่องที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคล
- ทำหน้าที่เป็นจุดติดต่อระหว่างหน่วยงานกำกับดูแลและผู้มีส่วนได้เสีย

เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) จะต้องปฏิบัติหน้าที่โดยคำนึงถึงความเสี่ยงที่เกี่ยวข้องกับการดำเนินการประมวลผลข้อมูล
โดยพิจารณาถึงลักษณะ ขอบเขต บริบท และวัตถุประสงค์ของการประมวลผลข้อมูลดังกล่าวอย่างรอบคอบ

แผนกเทคโนโลยีสารสนเทศ

แผนกเทคโนโลยีสารสนเทศ (IT)
มีหน้าที่รับผิดชอบในการดำเนินการมาตรการด้านความมั่นคงปลอดภัยทั้งทางเทคนิคและเชิงองค์กรให้เหมาะสมกับระดับความเสี่ยงของการประมวลผลข้อมูลส่วนบุคคล โดยสอดคล้องกับหลักการทั้งหมดที่ระบุไว้ในนโยบายฉบับนี้

6. นโยบาย

กิจกรรมแทบทุกอย่างที่ Grifols ดำเนินการล้วนเกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคลจากผู้มีส่วนได้เสียหลากหลายกลุ่ม ไม่ว่าจะเป็นพนักงาน ผู้ป่วย บุคลากรทางการแพทย์ ลูกค้า นักลงทุน ผู้ขาย และผู้บริจาค เป็นต้น

Grifols เคารพสิทธิความเป็นส่วนตัวของบุคคลทุกคนที่มอบข้อมูลส่วนบุคคลให้กับบริษัท และมีความมุ่งมั่นที่จะปฏิบัติตามข้อบังคับด้านความเป็นส่วนตัวที่เกี่ยวข้องทุกประการ.

ความมุ่งมั่นของ Grifols ต่อความโปร่งใส ความซื่อสัตย์ และหลักการต่าง ๆ ที่ระบุไว้ในเอกสารฉบับนี้ มีขอบเขตกว้างไกลเกินกว่าการปฏิบัติตามกฎระเบียบเพียงเท่านั้น Grifols ส่งเสริมวัฒนธรรมแห่งความเป็นส่วนตัวและการคุ้มครองข้อมูลโดยการสร้างความตระหนักรู้ให้แก่พนักงานเกี่ยวกับความหมายและวิธีการปกป้องข้อมูลส่วนบุคคล รวมถึงการนำแนวทางความเป็นส่วนตัวโดยการออกแบบและความเป็นส่วนตัวโดยค่าเริ่มต้นมาใช้ที่ Grifols ด้วยแนวทางนี้ Grifols สามารถสร้างความสัมพันธ์ที่ตั้งอยู่บนความไว้วางใจกับผู้มีส่วนได้เสีย และลดความเสี่ยงจากการละเมิดข้อมูลส่วนบุคคล รวมถึงความเสียหายต่อชื่อเสียงและผลกระทบทางเศรษฐกิจที่อาจเกิดขึ้น อันเป็นการส่งเสริมการเติบโตอย่างยั่งยืนในระยะยาวของ Grifols และสะท้อนถึงความมุ่งมั่นที่บริษัทมีต่อสังคม

6.1. หลักการคุ้มครองข้อมูลส่วนบุคคล

พนักงานทุกคนของ Grifols ที่มีหน้าที่ประมวลผลข้อมูลส่วนบุคคลต้องปฏิบัติตามนโยบายฉบับนี้ และยึดถือหลักการต่อไปนี้ในการดำเนินงาน:

a. <u>ประมวลผลข้อมูลส่วนบุคคลอย่างถูกต้องตามกฎหมาย เป็นธรรม และโปร่งใส</u> พนักงานควรตรวจสอบให้แน่ใจอยู่เสมอว่า Grifols มีฐานทางกฎหมายที่เหมาะสมและเพียงพอในการประมวลผลข้อมูลส่วนบุคคลของแต่ละบุคคล โดยทั่วไป ฐานทางกฎหมายจะถูกกำหนดไว้ในกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล ซึ่งรวมถึงแต่ไม่จำกัดเพียง การประมวลผลข้อมูลส่วนบุคคลเพื่อการปฏิบัติตามสัญญา (เช่น สัญญาจ้างงาน) การปฏิบัติตามข้อผูกพันทางกฎหมายที่เกี่ยวข้อง (เช่น การแจ้งข้อมูลส่วนบุคคลให้แก่หน่วยงานด้านภาษี) หรือเนื่องจากผลประโยชน์โดยชอบด้วยกฎหมายของ Grifols ทั้งนี้ ต้องอยู่ภายใต้เงื่อนไขว่าผลประโยชน์ดังกล่าวจะต้องไม่มีนัยสำคัญเกินกว่าสิทธิและเสรีภาพของเจ้าของข้อมูล (เช่น การป้องกันการฉ้อโกง) ตามที่กำหนดไว้ในกฎหมายคุ้มครองข้อมูลส่วนบุคคลที่เกี่ยวข้อง เจ้าของข้อมูลจะต้องได้รับแจ้งล่วงหน้าเกี่ยวกับวิธีการที่ข้อมูลส่วนบุคคลของตนจะถูกประมวลผล ผู้ที่รับผิดชอบในการประมวลผลข้อมูล และบุคคลหรือหน่วยงานที่ข้อมูลอาจถูกเปิดเผยให้ทราบ รวมถึงรายละเอียดอื่น ๆ ที่เกี่ยวข้อง

b. <u>เก็บรวบรวมข้อมูลส่วนบุคคลเฉพาะเพื่อวัตถุประสงค์ที่ระบุไว้โดยชัดเจน เฉพาะเจาะจง และชอบด้วยกฎหมายเท่านั้น</u> พนักงานมีสิทธิ์เก็บรวบรวมข้อมูลส่วนบุคคลได้เฉพาะเพื่อวัตถุประสงค์ที่ชัดเจน เฉพาะเจาะจง และชอบด้วยกฎหมายเท่านั้น และไม่สามารถนำข้อมูลส่วนบุคคลไปใช้เพื่อวัตถุประสงค์อื่นที่ไม่ได้แจ้งให้เจ้าของข้อมูลทราบล่วงหน้าได้ การเปลี่ยนแปลงวัตถุประสงค์ในการประมวลผลข้อมูลจะต้องมีการแจ้งให้เจ้าของข้อมูลทราบล่วงหน้า และอาจจำเป็นต้องมีฐานทางกฎหมายที่แตกต่างออกไปรองรับ รวมถึงอาจต้องได้รับความยินยอมจากเจ้าของข้อมูลด้วย

c. <u>ประมวลผลเฉพาะข้อมูลส่วนบุคคลที่มีความเหมาะสม สอดคล้อง และจำกัดเฉพาะเท่าที่จำเป็นตามวัตถุประสงค์ของการประมวลผลเท่านั้น (การลดปริมาณข้อมูล)</u> พนักงานจะต้องประมวลผลเฉพาะข้อมูลส่วนบุคคลในปริมาณที่น้อยที่สุดเท่าที่จำเป็นสำหรับวัตถุประสงค์เฉพาะที่ได้แจ้งแก่เจ้าของข้อมูลไว้เท่านั้น หากไม่จำเป็นต้องใช้ข้อมูลส่วนบุคคลหรือข้อมูลส่วนบุคคลบางประเภท ก็ไม่ควรมีการร้องขอหรือประมวลผลข้อมูลเหล่านั้นแต่อย่างใด

d. <u>ประมวลผลเฉพาะข้อมูลส่วนบุคคลที่ถูกต้องและเป็นปัจจุบันเท่านั้น</u> พนักงานจะต้องดำเนินการตามสมควรทุกประการเพื่อให้มั่นใจว่าข้อมูลส่วนบุคคลที่ประมวลผลนั้นถูกต้องและเป็นปัจจุบันตลอดวงจรชีวิตของข้อมูล (ตั้งแต่การเก็บรวบรวมจนถึงการทำลาย) ในเรื่องนี้ พนักงานจะต้องพยายามอย่างเต็มที่ตามสมควรในการแก้ไขหรือลบข้อมูลส่วนบุคคลที่ไม่ถูกต้องโดยทันที การดำเนินการดังกล่าวอาจต้องอาศัยความร่วมมือและการมีส่วนร่วมจากหลายหน่วยงานภายใน Grifols ตามที่ระบุไว้ในนโยบายและระเบียบปฏิบัติที่เกี่ยวข้อง

e. <u>เก็บรักษาข้อมูลส่วนบุคคลไว้ในระยะเวลาที่จำเป็นตามวัตถุประสงค์ของการประมวลผล และตามที่กฎหมายกำหนดเท่านั้น</u> พนักงานจะต้องเก็บรักษาข้อมูลส่วนบุคคลไว้ในแฟ้มข้อมูลของ Grifols (ทั้งในรูปแบบอิเล็กทรอนิกส์และเอกสารกระดาษ) เฉพาะในช่วงเวลาที่จำเป็นต่อการบรรลุวัตถุประสงค์ของการประมวลผลข้อมูลนั้น หรือในกรณีที่กฎหมายกำหนดให้ต้องเก็บรักษาไว้เท่านั้น พนักงานจะต้องดำเนินการตามสมควรทุกประการเพื่อลบข้อมูลส่วนบุคคลเมื่อไม่มีความจำเป็นต้องเก็บรักษาข้อมูลนั้นไว้อีกต่อไป การดำเนินการดังกล่าวอาจต้องอาศัยความร่วมมือและการมีส่วนร่วมจากหลายหน่วยงานภายใน Grifols ตามที่ระบุไว้ในนโยบายและระเบียบปฏิบัติที่เกี่ยวข้อง

f. ประมวลผลข้อมูลส่วนบุคคลด้วยวิธีการที่ปลอดภัย Grifols
จะนำมาตรการด้านความปลอดภัยทั้งในระดับองค์กรและทางเทคนิคมาใช้เพื่อปกป้องข้อมูลส่วนบุคคล รับรองความลับ ความพร้อมใช้งาน และจะดำเนินการแบ่งปันข้อมูลดังกล่าวอย่างปลอดภัยตามที่กฎหมายและข้อบังคับกำหนดในกรณีที่จำเป็น
พนักงานทุกคนของ Grifols
จะต้องปฏิบัติตามมาตรการด้านความปลอดภัยทางเทคนิคและระดับองค์กรที่เกี่ยวข้องอย่างเคร่งครัด
โดยมาตรการเหล่านี้มีความสำคัญเป็นพิเศษเมื่อมีการประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหวหรืออยู่ในหมวดหมู่พิเศษ

6.2. สิทธิของเจ้าของข้อมูลต่อข้อมูลส่วนบุคคลของตนเอง

กฎหมายคุ้มครองข้อมูลส่วนบุคคลมอบสิทธิหลายประการให้แก่บุคคล เช่น การเข้าถึงข้อมูลส่วนบุคคลของตนเอง
การขอให้ข้อมูลส่วนบุคคลที่ไม่ถูกต้องได้รับการแก้ไข หรือการขอให้ลบข้อมูลส่วนบุคคลของตนเอง เป็นต้น
สิทธิเหล่านี้และวิธีการที่บุคคลสามารถใช้สิทธิเหล่านั้นได้ถูกระบุไว้อย่างชัดเจนในประกาศความเป็นส่วนตัวของ Grifols
ที่จัดเตรียมให้แก่บุคคล

ตามกฎหมายที่เกี่ยวข้อง สิทธิของบุคคลต่อข้อมูลส่วนบุคคลของตนเองอาจรวมถึงสิทธิดังต่อไปนี้:

- ข้อมูล: สิทธิในการได้รับข้อมูลที่กระชับ โปร่งใส สามารถเข้าใจได้ง่าย และเข้าถึงได้ง่ายเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคล
  โดยทั่วไปแล้ว Grifols จะจัดเตรียมข้อมูลนี้ในประกาศความเป็นส่วนตัว
  ซึ่งรวมถึงรายละเอียดการติดต่อของผู้ควบคุมข้อมูลและเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล วัตถุประสงค์และฐานทางกฎหมาย (เหตุผล) สำหรับการประมวลผล ประเภทของผู้รับข้อมูล (ถ้ามี) ระยะเวลาการเก็บรักษาข้อมูลส่วนบุคคล
  และสิทธิในการคุ้มครองข้อมูลที่กล่าวถึงด้านล่าง เป็นต้น เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)
  และที่ปรึกษากฎหมายของ Grifols ร่วมกับพนักงานจะเป็นผู้จัดทำและ/หรือทบทวนประกาศความเป็นส่วนตัวตามความจำเป็น
- การเข้าถึง: สิทธิในการขอการยืนยันว่า มีการประมวลผลข้อมูลส่วนบุคคลหรือไม่ และหากมีการประมวลผล
  สามารถขอเข้าถึงข้อมูลส่วนบุคคลที่เก็บอยู่ในแฟ้มข้อมูลของ Grifols ได้
- การแก้ไข: สิทธิในการขอให้ทำการแก้ไขข้อมูลส่วนบุคคลที่ไม่ถูกต้อง
- การลบข้อมูล: สิทธิในการขอให้ลบข้อมูลส่วนบุคคล
- การคัดค้าน: สิทธิในการขอให้ข้อมูลส่วนบุคคลไม่ได้รับการประมวลผลในกรณีเฉพาะ
- ความสามารถในการพกพา: สิทธิในการขอรับข้อมูลส่วนบุคคลที่ให้แก่ Grifols ในรูปแบบไฟล์อิเล็กทรอนิกส์
  และสิทธิในการถ่ายโอนข้อมูลดังกล่าวไปยังบุคคลอื่น
- การจำกัดการประมวลผล: สิทธิในการขอให้มีการจำกัดการประมวลผลข้อมูลส่วนบุคคลเมื่อ:
  i. มีการตรวจสอบความถูกต้องของข้อมูลส่วนบุคคลหลังจากที่มีการโต้แย้ง
  ii. การประมวลผลข้อมูลส่วนบุคคลเป็นการกระทำที่ผิดกฎหมาย และเจ้าของข้อมูลคัดค้านการลบข้อมูลนั้น
  iii. Grifols ไม่ต้องการข้อมูลส่วนบุคคลสำหรับวัตถุประสงค์ของการประมวลผลอีกต่อไป
  แต่เจ้าของข้อมูลต้องการข้อมูลนั้นสำหรับการจัดตั้ง การใช้ หรือการปกป้องข้อเรียกร้องทางกฎหมาย และ
  iv. เจ้าของข้อมูลได้คัดค้านการประมวลผลข้อมูลที่อ้างอิงจากผลประโยชน์สาธารณะหรือผลประโยชน์โดยชอบของ Grifols
  ขณะที่กำลังตรวจสอบว่าเหตุผลที่ชอบด้วยกฎหมายของ Grifols มีน้ำหนักมากกว่าของเจ้าของข้อมูลหรือไม่
- การเพิกถอนความยินยอม: สิทธิในการเพิกถอนความยินยอมที่ได้ให้ไว้
  โดยไม่กระทบต่อความชอบด้วยกฎหมายของการประมวลผลที่อาศัยความยินยอมก่อนที่จะมีการเพิกถอน

Grifols จัดตั้งกระบวนการภายในเพื่ออำนวยความสะดวกและจัดการการใช้สิทธิด้านการคุ้มครองข้อมูลของบุคคล พนักงานของ Grifols
ที่ได้รับคำขอการใช้สิทธิจากเจ้าของข้อมูลส่วนบุคคลจะต้องติดต่อทันทีไปยังบุคคลหรือหน่วยงานที่รับผิดชอบด้านการคุ้มครองข้อมูลภายในองค์กรของตน หรือหากไม่มีให้ติดต่อไปยัง *Corporate Data Protection Office* (privacy@grifols.com)

6.3. การเก็บรักษาข้อมูลส่วนบุคคล

เมื่อไม่จำเป็นต้องใช้ข้อมูลส่วนบุคคลสำหรับวัตถุประสงค์ที่กำหนดในการประมวลผลหรือเพื่อปฏิบัติตามข้อผูกพันทางกฎหมายที่เกี่ยวข้อง
โดยพนักงานจะต้องดำเนินการตามสมควรทุกประการเพื่อทำลายหรือลบสำเนาของข้อมูลส่วนบุคคลทั้งหมด ไม่ว่าจะอยู่ในรูปแบบกระดาษ
หรือในการจัดเก็บข้อมูลทางกายภาพหรือดิจิทัลอื่นใด

โปรดดูข้อมูลเพิ่มเติมเกี่ยวกับหัวข้อนี้ที่นโยบายการเก็บรักษาข้อมูลของ Grifols (*"Records Retention Policy"* ID448)

6.4. ความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลและการละเมิดข้อมูลส่วนบุคคล

Grifols ดำเนินการจัดตั้งกระบวนการและเทคโนโลยีเพื่อรักษาความปลอดภัยของข้อมูลส่วนบุคคลตลอดระยะเวลาที่เก็บรักษา
โดยนำมาตรการทางเทคนิคและเชิงองค์กรที่สมเหตุสมผลมาใช้เพื่อรักษาความปลอดภัยของข้อมูลส่วนบุคคล
โดยให้ความสำคัญเป็นพิเศษกับข้อมูลส่วนบุคคลที่มีความอ่อนไหวหรืออยู่ในหมวดหมู่พิเศษ นอกจากนี้ Grifols
ยังได้กำหนดกระบวนการสำหรับการทดสอบ ประเมินผล และประเมินประสิทธิภาพของมาตรการเหล่านี้เป็นประจำ เพื่อให้มั่นใจว่า:

a. ความพร้อมใช้งานของข้อมูลส่วนบุคคล: ระบบข้อมูลทางธุรกิจและข้อมูลส่วนบุคคลสามารถใช้งานได้ตามลักษณะและเวลาที่ต้องการ Grifols ดำเนินการตามมาตรการที่สมเหตุสมผลเพื่อป้องกันการสูญหาย การทำลาย หรือความเสียหายที่เกิดขึ้นโดยไม่ตั้งใจหรือไม่ได้รับอนุญาต โดยสามารถกู้คืนข้อมูลส่วนบุคคลได้อย่างรวดเร็วในกรณีที่เกิดเหตุการณ์ทางกายภาพหรือทางเทคนิค

b. ความลับของข้อมูลส่วนบุคคล: ระบบและแฟ้มข้อมูลที่เก็บข้อมูลส่วนบุคคลจะได้รับการเข้าถึงโดยบุคคลที่ได้รับอนุญาตเท่านั้น เพื่อป้องกันการเข้าถึงหรือการเปิดเผยข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาต การเข้าถึงโดยไม่ได้ตั้งใจ หรือการเข้าถึงโดยไม่ชอบด้วยกฎหมาย

c. ความสมบูรณ์ของข้อมูลส่วนบุคคล:เพื่อรักษาความถูกต้องของข้อมูลส่วนบุคคลจากการเปลี่ยนแปลงโดยไม่ได้ตั้งใจหรือการเปลี่ยนแปลงที่เกิดจากการฉ้อโกง

พนักงานทุกคนต้องปฏิบัติตามนโยบายและระเบียบปฏิบัติด้านความปลอดภัยของข้อมูลที่เกี่ยวข้องของ Grifols เมื่อประมวลผลข้อมูลส่วนบุคคล ซึ่งรวมถึงแต่ไม่จำกัดเพียงนโยบายความปลอดภัยทางเทคโนโลยีสารสนเทศ

การละเมิดข้อมูลส่วนบุคคลเป็นเหตุการณ์ด้านความปลอดภัยประเภทหนึ่งที่ทำให้ความพร้อมใช้งาน ความลับ หรือความสมบูรณ์ของข้อมูลส่วนบุคคลถูกทำลายหรือถูกเปิดเผย Grifols ได้ออกแบบกระบวนการ (DPO-SOP-000001_Personal Data Incident Procedure) สำหรับพนักงานในการแจ้งเหตุการณ์ด้านความปลอดภัยและการละเมิดข้อมูลส่วนบุคคล เพื่อให้ Grifols สามารถดำเนินการประเมินความเสี่ยงและความปลอดภัยที่เกี่ยวข้อง และปฏิบัติตามข้อผูกพันในการแจ้งหน่วยงานคุ้มครองข้อมูลส่วนบุคคลและเจ้าของข้อมูลที่ได้รับผลกระทบในกรณีที่จำเป็น

6.5. การถ่ายโอนข้อมูลส่วนบุคคลและผู้ให้บริการ

ในระหว่างการดำเนินธุรกิจตามปกติ พนักงานอาจจำเป็นต้องทำสัญญาบริการและ/หรือถ่ายโอนข้อมูลส่วนบุคคลไปยังบริษัทในเครือของ Grifols หรือบุคคลภายนอกในหลายประเทศ เพื่อเหตุผลทางธุรกิจที่ชอบด้วยกฎหมาย หรือตามที่กฎหมายอนุญาตหรือกำหนดไว้

เมื่อจ้างบริการใหม่จากบุคคลภายนอก (ไม่ว่าจะเป็นผู้ขายรายเดิมหรือรายใหม่) ที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคล จะต้องดำเนินการประเมินผู้ขายเพื่อประเมินความเสี่ยงและผลกระทบของการประมวลผลนั้นต่อสิทธิและเสรีภาพของเจ้าของข้อมูล วัตถุประสงค์ของการประเมินคือการยืนยันว่าผู้ขายมีความสามารถในการปกป้องและประมวลผลข้อมูลส่วนบุคคลตามหลักการและมาตรฐานที่กำหนดในนโยบายฉบับนี้ รวมถึงข้อกำหนดของกฎหมายคุ้มครองข้อมูลส่วนบุคคลที่บังคับใช้

สัญญาบริการทั้งหมดกับบุคคลภายนอกหรือบริษัทในเครือของ Grifols ที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคลจะต้องมีการระบุข้อกำหนดด้านการคุ้มครองข้อมูล หรือการอ้างอิงถึงข้อตกลงการคุ้มครองข้อมูลที่ได้ลงนามแล้ว

การถ่ายโอนข้อมูลส่วนบุคคลข้ามพรมแดนสามารถทำได้เฉพาะเมื่อมีมาตรการป้องกันที่เหมาะสมเพื่อคุ้มครองข้อมูลส่วนบุคคลเหล่านั้น

Grifols ได้จัดตั้งกระบวนการภายในเพื่อยืนยันว่า การถ่ายโอนข้อมูลส่วนบุคคลข้ามพรมแดนและการจ้างบริการจากผู้ให้บริการเป็นไปตามข้อกำหนดของกฎหมายคุ้มครองข้อมูลส่วนบุคคลที่บังคับใช้

6.6. การฝึกอบรมและการสร้างความตระหนักรู้

Grifols มุ่งมั่นที่จะส่งเสริมวัฒนธรรมด้านความเป็นส่วนตัวที่เคร่งครัดภายในบริษัท Grifols ส่งเสริมและจัดฝึกอบรมที่เหมาะสมให้แก่พนักงาน โดยมีขนาดและความเหมาะสมตามการประมวลผลข้อมูลส่วนบุคคลที่พวกเขาดำเนินการ เพื่อสร้างความตระหนักรู้และให้การศึกษาเกี่ยวกับวิธีการระบุและจัดการข้อมูลส่วนบุคคลในลักษณะที่สอดคล้องกับมาตรฐานและระเบียบปฏิบัติของ Grifols รวมถึงข้อกำหนดด้านความเป็นส่วนตัวที่บังคับใช้

6.7. ความเป็นส่วนตัวโดยการออกแบบและความเป็นส่วนตัวโดยค่าเริ่มต้น

พนักงานควรพิจารณาด้านความเป็นส่วนตัวและการคุ้มครองข้อมูลตลอดวงจรชีวิตของข้อมูลส่วนบุคคล (ตั้งแต่การเก็บรวบรวมจนถึงการทำลาย) และจะต้องนำหลักการการคุ้มครองข้อมูลและมาตรการด้านความปลอดภัยมาใช้ในกิจกรรมทางธุรกิจภายใน Grifols โดยเฉพาะเมื่อมีการดำเนินโครงการใหม่ นอกจากนี้ มาตรการด้านความปลอดภัยทั้งทางเทคนิคและเชิงองค์กรที่เหมาะสมจะต้องได้รับการดำเนินการเพื่อให้มั่นใจว่าเฉพาะข้อมูลส่วนบุคคลที่จำเป็นที่สุดเท่านั้นที่จะได้รับการประมวลผล

7. สาเหตุของการเปลี่ยนแปลง

การปรับปรุงข้อมูลคำจำกัดความและเอกสารที่เกี่ยวข้อง