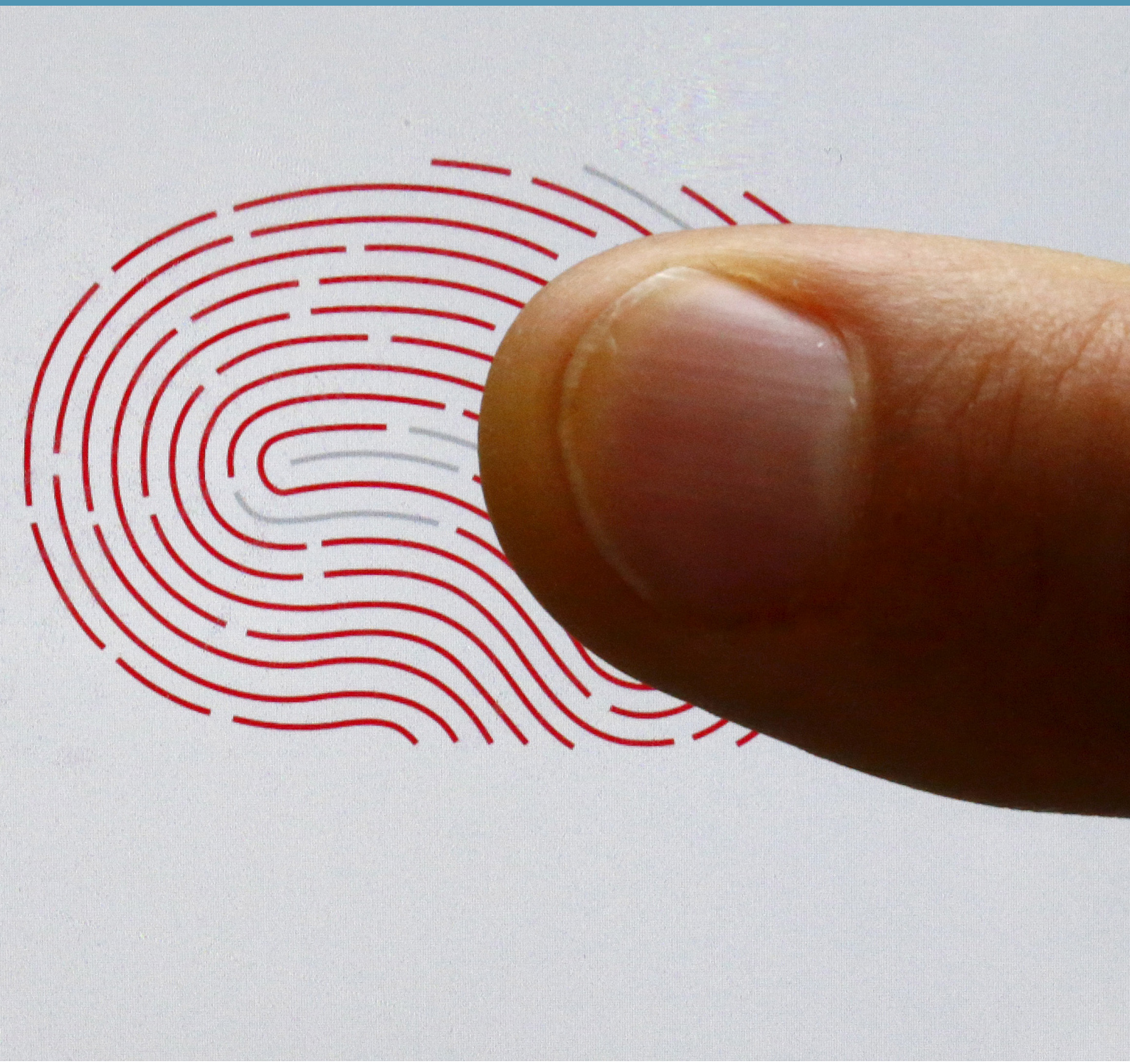
Impacto de la nueva regulación europea de datos personales a las ONGs en América Latina

Impact of the EU General Data Protection Regulation on NGOs in Latin America



RCTZZ ABOGADOS
Richards Cardinal Tützer Zabala Zaefferer

THOMSON REUTERS FOUNDATION

RECONOCIMIENTO
/ACKNOWLEDGEMENTS

RCTZZ ABOGADOS
RICHARDS CARDINAL TÜTZER ZABALA ZAEFFERER

Richards, Cardinal, Tützer Zabala & Zaefferer

THOMSON REUTERS FOUNDATION

Thomson Reuters Foundation

DESCARGO DE RESPONSABILIDAD /DISCLAIMER

Este documento y la información que contiene se proporcionan únicamente con fines informativos generales. Se han preparado como una herramienta para informar a las ONGs sobre la existencia de una nueva reglamentación sobre datos personales europea que puede afectarlos. No representa un asesoramiento jurídico con respecto a las leyes de ninguna jurisdicción y no pretende identificar las necesidades legales de su organización. No constituye y no debe ser utilizado como consejo legal o crear una relación abogado-cliente con Richards, Cardinal, Tützer, Zabala & Zaefferer o la Fundación Thomson Reuters. Ni la Fundación Thomson Reuters ni el estudio Richards, Cardinal, Tützer, Zabala & Zaefferer aceptan ninguna responsabilidad por las pérdidas que puedan derivarse de la referencia a la información contenida en este documento o cualquier inexactitud en la misma. El asesoramiento jurídico debe obtenerse de un asesor legal calificado en la(s) jurisdicción(es) relevante(s) cuando se trate de circunstancias específicas.

This document, and the information it contains, is provided for general informational purposes only. It has been prepared as a tool to inform NGOs of the existence of a new EU personal data regulation that may affect them. It does not represent legal advice in respect of the laws of any jurisdiction and it does not purport to identify the legal needs of your organisation. It does not constitute, and must not be relied or acted upon as, legal advice or create an attorney-client relationship with Richards, Cardinal, Tützer, Zabala & Zaefferer or the Thomson Reuters Foundation. Neither the Thomson Reuters Foundation nor the firm, Richards, Cardinal, Tützer, Zabala & Zaefferer, accept any responsibility for losses that may arise from reliance upon the information contained in this document or any inaccuracies therein. Legal advice should be obtained from legal counsel qualified in the relevant jurisdiction(s) when dealing with specific circumstances.

SOBRE NOSOTROS
/ABOUT US

La **Fundación Thomson Reuters** apoya al periodismo libre e independiente, los derechos humanos, el empoderamiento de las mujeres y el estado de derecho. Utilizamos las habilidades, los valores y la experiencia de Thomson Reuters para ejecutar programas que impulsan el cambio real y empoderan a la gente en todo el mundo, incluyendo la asistencia legal gratuita, la capacitación en medios de comunicación y periodismo, la cobertura de historias poco reportadas alrededor del mundo y la conferencia Trust Conference.

TrustLaw es el programa global de pro bono legal de la Fundación Thomson Reuters, que conecta a las mejores firmas de abogados y equipos jurídicos corporativos de todo el mundo con ONGs de alto impacto y empresas sociales que trabajan para crear un cambio social y ambiental. Producimos investigación jurídica novedosa y ofrecemos cursos de capacitación innovadores en todo el mundo.

The **Thomson Reuters Foundation** stands for free, independent journalism, human rights, women's empowerment and the rule of law. We use the skills, values and expertise of Thomson Reuters to run programmes that trigger real change and empower people around the world, including free legal assistance, journalism and media training, coverage of the world's underreported stories, and the Trust Conference.

TrustLaw is the Thomson Reuters Foundation's global pro bono legal programme, connecting the best law firms and corporate legal teams around the world with high-impact non-governmental organisations and social enterprises working to create social and environmental change. We produce ground-breaking legal research and offer innovative training courses worldwide.

CONTENIDOS /CONTENTS

LA GUÍA
THE GUIDE

¿QUÉ ES GDPR?

Es el Reglamento General de Protección de Datos (GDPR) de la Unión Europea, en vigencia desde el 25/5/2018 y regula el tratamiento de datos de individuos residentes de la Unión Europa. Debido a su alcance extraterritorial, GDPR aplica a aquellas entidades –independientemente de donde se encuentren físicamente ubicadas o legalmente radicadas-, que de alguna manera usen o procesen información personal relacionada con individuos residentes en la Unión Europea.

Las ONGs ubicadas en América Latina que usen o procesen datos de residentes europeos deberían cumplir con un doble régimen: (1) Las leyes de datos personales del país de América Latina donde se encuentren radicadas; y (2) GDPR.

WHAT IS GDPR?

It is the General Data Protection Regulation (GDPR) of the European Union, in force since 05/25/2018 that regulates the treatment of data of residents of the European Union. Due to its extraterritorial scope, the GDPR applies to those entities - regardless of where they are physically or legally located - that in some way use or process personal information related to individuals residing in the European Union.

NGOs located in Latin America that use or process data from European residents should comply with a double regime: (1) The personal data laws of the country of Latin America where they are located; and (2) GDPR.

CONCEPTOS BÁSICOS DE GPDR

- **"Datos personales"**: Toda información sobre una persona física, identificada u identificable. El nombre, documento de identidad, profesión, dirección de email, o sexo de una persona, son ejemplos de datos personales.

- **"Tratamiento de datos"**: Cualquier tipo de operación(es) realizada(s) sobre datos personales como, por ejemplo: recopilación, almacenamiento, envio cesión, utilización de datos, entre muchas otras. Remitir un email, recabar datos para una encuesta o enviar publicidad a destinatarios son ejemplos de operaciones de tratamiento de datos.

- **"Responsable"**: es la persona o empresa que determina los fines y medios del tratamiento de datos (cómo y para qué se van a usar). La ONG que en base a datos personales recolectados determina un programa de ayuda social es la "responsable" del tratamiento de datos.

BASIC CONCEPTS OF GPDR

- **"Personal Data"**: All information about a natural person, identified or identifiable. The name, ID, profession, email address, or gender of a person, are examples of personal data.

- **"Data processing"**: Any type of operation(s) performed on personal data, such as: collection, storage, sending, transfer, use of data, among many others. Sending an email, collecting data for a survey or sending advertisements to recipients are examples of data processing operations.

- **"Responsible/Controller"**: is the person or company that determines the purposes and means of data processing (how and for what it is going to be used). The NGO that uses personal data to design a social assistance program, for example, is "responsible" for the data processing.

- **"Encargado"**: es la persona o empresa que trata datos personales por cuenta del responsable del tratamiento. La agencia de marketing, el contador o la empresa de informática que trabajan para la ONG y manejan datos provistos por la ONG, son "encargados" porque tratan esos datos por cuenta de la ONG.

APLICACIÓN DE GPDR A ONGS FUERA DE LA UNIÓN EUROPEA

Uno de los aspectos más salientes y novedosos de GDPR es que, en razón del principio de extraterritorialidad, aplica a cualquier entidad – incluyendo ONGs- que traten datos de residentes europeos, aun cuando tales entidades se encuentren fuera de la Unión Europea.

En este sentido, GDPR podría ser aplicable a cualquier ONG ubicada en cualquier país que esté fuera de la UE y de cualquier tamaño (pequeñas, medianas, grandes). Por lo tanto, el GDPR aplicará:

i. a todas las ONGs que traten datos de residentes de la UE;
ii. aquellas que monitoreen conductas de residentes de la UE; y
iii. ofrezcan productos o servicios a residentes de la UE.

En pocas palabras, **el GDPR tiene un impacto potencial en cualquier ONG del mundo que realice tratamiento de datos de residentes de la UE, independientemente del país en donde esté radicada la ONG; de si la ONG es grande o chica; de la cantidad de empleados que tenga la ONG; o del volumen de facturación/recaudación de la ONG.**

Ejemplos simples de aplicación de GDPR:

- ONG de América Latina recibe donaciones de personas residentes de la UE;

- **"In charge/Processor"**: is the person or company that processes personal data on behalf of the controller. The marketing agency, the accountant or the IT company that works for the NGO and manages data provided by the NGO, are "in charge" because they process this data on behalf of the NGO.

APPLICATION OF GDPR TO NGOS OUTSIDE THE EUROPEAN UNION

One of the most relevant and novel aspects of GDPR is that, because of the principle of extraterritoriality, it applies to any entity -including NGOs- that process data of European residents, even when such entities are outside the European Union.

In this sense, GDPR could be applicable to any NGO located in any country that is outside the EU and of any size (small, medium or large). Therefore, the GDPR will apply:

i. to all NGOs that process EU residents' data;
ii. those that monitor behaviors of EU residents; and
iii. offer products or services to EU residents.

In summary, **GDPR will impact any NGO in the world that conducts data processing of EU residents, regardless of the country where the NGO is located; if the NGO is big or small; of the number of employees that the NGO has; or the turnover / funding of the NGO.**

Simple examples of the application of GDPR:

- NGO from Latin America receives donations from EU residents;

- actividades a residentes de la UE;
- ONG de América Latina intercambia datos con su afiliada en la UE;
- ONG de América Latina procesa datos de residentes de la UE para realizar programas sociales.

- NGO from Latin America exchanges data with its affiliate in the EU;
- NGO from Latin America processes data of EU residents to run social programs.

GDPR establece fuertes **multas** por incumplimientos, que pueden llegar a 10.000.000 de Euros o hasta el 2% del monto total de negocios global correspondiente al ejercicio financiero de la empresa infractora, o incluso a 20.000.000 de Euros o hasta el 4% del monto global antedicho en ciertos casos graves.

Amén de estas sanciones legales, una sanción 'de facto' podría ser que empresas o personas europeas se nieguen a vincularse con entidades que incumplan GDPR cuando les resulta aplicable.

GDPR establishes hefty **fines** for non-compliance, which can reach 10,000,000 Euros or up to 2% of the total global business amount corresponding to the financial year of the infringing company, or even 20,000,000 Euros or up to 4% of the above-mentioned global amount in certain severe cases.

In addition to these legal sanctions, a 'de facto' penalty could be that European companies or individuals refuse to associate with entities that fail to comply with GDPR when applicable.

NUEVOS DERECHOS RECONOCIDOS POR GDPR

Más allá de los ya típicos derechos de acceso, rectificación, cancelación y oposición (Derechos 'ARCO'), GDPR reconoce a favor de los titulares de los datos nuevos derechos, como el 'derecho al olvido', el derecho a la portabilidad de los datos o el derecho de oponerse al tratamiento con fines específicos. También establece nuevas obligaciones para los responsables de los datos (es decir, las ONG), como por ejemplo denunciar en un breve plazo cualquier incidente de seguridad de datos personales (es decir, hackeo o acceso no autorizado), la obligación de designar a un representante a los fines del GDPR con asiento físico en la Unión Europea; de designar un agente de protección de datos personales en ciertos casos; y cláusulas obligatorias que deben incluirse –y cumplirse- en contratos con proveedores.

NEW RIGHTS RECOGNIZED BY GDPR

Beyond the usual rights of access, rectification, cancellation and opposition ('ARCO' rights), GDPR recognizes new data rights in favor of data owners, such as the 'right to be forgotten', the right to portability of data or the right to object to a process for specific purposes. It also establishes new obligations for those responsible for the data (i.e. NGOs), such as: reporting any breach of personal data security (i.e. hacking or unauthorized access) in the short term; the obligation to appoint a representative with a physical presence in the European Union for the purposes of GDPR; to designate a personal data protection agent in certain cases; and to insert mandatory clauses that must be included -and fulfilled- in contracts with suppliers.

QUÉ HACER

El **consentimiento** del interesado (titular del dato) es el principio básico del que debe partirse en materia de datos personales. Siempre que maneje datos personales, debería preguntarse: ¿Cómo obtuve estos datos? ¿El titular de los datos me dio su permiso para usarlos? ¿Tengo permiso para usarlos? ¿Los estoy usando para la finalidad para la cual el titular dio su permiso? ¿A quién/es se los estoy dando?

Tomando este principio –que seguramente servirá como premisa básica para cumplir con la ley de datos personales del país de cada ONG- cabe preguntarse cómo prepararse para cumplir con GDPR, si es que su ONG procesa datos de personas de la UE. Un modo de comenzar podría ser el siguiente:

- **Realice un análisis**. Lo más razonable sería consultar a un experto en protección de datos personales para determinar qué regulaciones impactan a su ONG, de qué modo se recolectan y procesan actualmente los datos personales en su ONG, cuál es su estatus actual, y qué puntos debería cambiar o mejorar.

- **Concientice a su personal** sobre qué implicancias tiene el manejo de datos personales y datos sensibles, y qué consecuencias (sanciones legales, reputacionales, de negocio, etc.) puede generar el incumplimiento de la normativa aplicable.

- **Designe a una persona responsable** (puede ser de dentro o fuera de la ONG) que verifique la correcta protección de los datos personales que su ONG trata y evacué las dudas que se presente en la operación diaria.

- **Categorice los datos que se recopilan**, así como su acceso y su procesamiento. Si se trata o no de datos "sensibles", a residentes de qué país/es pertenece/n, quienes tienen acceso a los mismos, etc.

WHAT TO DO

The **consent** of the interested party (data owner) is the basic principle from which the personal data processor must start. Whenever you handle personal data, you should ask yourself: How did I obtain this data? Did the data owner give me permission to use them? Do I have permission to use it? Am I using it for the purpose for which the owner gave his permission? Who am I giving the data to?

Taking this principle -which will likely serve as a basic premise to comply with the personal data law of the country of each NGO- you may ask yourself how to prepare to comply with GDPR, if your NGO processes data from people in the EU. A way to start could be following these steps:

- **Run an analysis.** The most reasonable thing would be to consult an expert in personal data protection to determine what regulations impact your NGO, how personal data is currently collected and processed at your NGO, what is its current status, and what points should be changed or improved.

- **Educate your staff** about the implications of handling personal data and sensitive data, and what consequences (legal, reputational, business sanctions, etc.) can non-compliance with applicable regulations cause.

- **Designate a responsible person** (can be from inside or outside the NGO) to verify the correct protection of the personal data that your NGO processes and remove any doubts that might arise in daily operations.

- **Categorize the data that is collected**, as well as its access and processing. For example, you can determine whether or not it is "sensitive" data, which countries the data owners are from, who has access to the data, etc.

- **Revise los contratos de su ONG con proveedores o terceros** que puedan encontrarse sujetos a la regulación del GDPR, para determinar que contengan las cláusulas y requerimientos de GDPR y de la normativa de datos personales de su país; y si sus proveedores también cumplen con la normativa (ya que, en caso negativo, su ONG podría terminar siendo la responsable).

- **Review the contracts of your NGO with suppliers or third parties** that may be subject to the GDPR regulation, to determine whether they contain GDPR clauses and requirements and the regulations applicable to personal data in your country. You should also review whether your suppliers need to comply with the regulations (because if not, your NGO could end up being responsible).