European Union's General Data Protection Regulation (GDPR)

Frequently Asked Questions

The following information is being provided by Isagenix to assist our Associates in better understanding how GDPR may impact their independent businesses. It is not a complete guide to the law and does not constitute legal advice.

What is GDPR?
GDPR is the acronym for the General Data Protection Regulation, a binding legislative act which became effective May 25, 2018. It unifies the data protection laws across the entire EU and is designed to protect data and privacy of all EU residents, wherever the information is individuals used throughout the world. GDPR includes additional regulations regarding the use of information that is exported outside the EU.

Is Isagenix in compliance with GDPR?
Yes. For over a year, a cross-department team and outside legal counsel have been working to prepare Isagenix for GDPR. The goals of GDPR align with our company's data security objectives whereby we continually seek to ensure the confidentiality, integrity and availability of the personal data we store or process. We maintain appropriate technical and organizational security measures to protect personal data against accidental or unlawful destruction or loss, alteration, unauthorised disclosure or access.

Since Isagenix is already responsible for complying with GDPR, doesn't that also cover me?
Not entirely. Since Associates are independent contractors, you are responsible for complying with GDPR as to your use and maintenance of personal data of EU residents. Isagenix is responsible for complying with GDPR for information maintained on our systems. However, once you access personal information, either directly through Isagenix systems or through your own data collection and record maintenance, you are accountable for protecting the data and using it responsibly. Therefore, it is important that you become familiar with GDPR and follow the procedures to ensure you comply the regulations.

Where can I find more information about GDPR?
Data Protection Authorities (DPAs) in each EU country are responsible for enforcing the GDPR. If a business does not comply with GDPR obligations, the applicable DPA(s) can give issue a warning, suspend or ban data-processing activities, or impose fines. A list of DPA website addresses and other contact information for each EU country can be found here. Additional information about can be found here.

Will GDPR make it difficult for me to do business in the EU?
Not if you follow sound business practices. While it may sound intimidating, GDPR is about treating other people's personal information with care and respect. These FAQs are intended to help you navigate GDPR regulations and provide some basic guidance to help your business.

Should I pay attention to GDPR if I am not an EU citizen?
Yes. GDPR applies to any person or entity that does business with EU residents and/or holds or processes the personal data of EU residents. Therefore, if you have customers or team members who reside in the EU, you must comply with GDPR. Under GDPR, you are responsible for the protection of information you choose to maintain regarding your customers and team members.

(Continued)

Do I need to register or pay a fee?
That depends on your business. You should review the DPA websites for each country where you conduct business to determine if registration or fees are required. For example, if you do business in the UK, check here to complete an assessment to determine if you need to pay a fee. Failure to pay a required fee will result in a fixed penalty, so be sure to take this assessment right away.

What should I do if I believe information regarding my Isagenix business is, or may have been compromised?
If you believe someone has accessed your Isagenix account or any Isagenix system that contains your personal information or that of your customers or team members, contact Isagenix's Data Protection Officer immediately at privacyeu@isagenixcorp.com. If the security breach involves UK residents, you may need to file a report with the ICO within 72 hours by calling the ICO helpline at 0303 123 1113 or online.

Are there some general guidelines that I should follow regarding the protection of personal information of my customers and team members?
While Isagenix can't provide legal advice to independent Associates, here are some good business practices that you should follow for ALL of your operations, anywhere in the world, to protect you, your customers and team members. These guidelines include:

- Make sure your own personal information in Isagenix systems is accurate and up-to-date, including information in the ABO or any other Isagenix-provided website, app or system.
- Always have your customers enter their own account information into Isagenix systems. Not only will this protect their privacy, it will help ensure the accuracy of both their personal information, product preferences and payment and delivery options.
- Treat all personal information as if it's a large pile of money – it's valuable! For example:
    - Don't leave personal information where it can be compromised or stolen!
    - Protect the confidentiality of personal information and avoid a security breach that may result in unintended destruction, loss, change, disclosure or access of data, either mistakenly, or deliberately and illegally.
- If you collect information offline, treat it with the same care as you would digital data.
- Always be open and transparent with others about how you'll use their information, whether you receive the information directly from them or from another source. Be sure you confirm that they approve the use of their information and obtain their written consent (particularly when dealing with EU residents since GDPR requires proof of consent). And, don't use personal information for any purpose other than for what you have received specific consent.
- Respect others' choices – if they don't want you to contact them, then don't. If they ask you to stop contacting them after previously giving their consent, don't continue to contact them or try to convince them to stay connected. Remember that consent can be withdrawn at any time so always be respectful of requests to remove information from your records. Under GDPR, you must honor these requests within 1 month.
- Be careful not to inadvertently violate someone's privacy. For instance, it's appropriate to update your customer's data if they personally provide this new information; however, it isn't proper to seek such data indirectly, since they may not wish for you to have it.