



Global Data Protection Policy

EFFECTIVE FEBRUARY 2018

ENGLISH

ARABIC

BAHASA INDONESIA

BAHASA MALAY

CHINESE (SIMPLIFIED)

DUTCH

FRENCH (CANADA)

FRENCH (EUROPEAN)

GERMAN

ITALIAN

KOREAN

POLISH

PORTUGUESE (BRAZIL)

RUSSIAN

SPANISH (LATIN AMERICA)



Global Data Protection Policy

Effective Date: February 2018

Last Revision: April 2025

Section 1: Purpose of this Policy

This Global Data Protection Policy (the "Policy") promotes an effective balance between information security practices and business needs, while maintaining compliance with relevant laws. The Policy helps Energizer meet our legal obligations while maintaining the ability for the business to be agile and meet customer expectations. As set forth below in more detail, Energizer requires different levels of security controls depending on the classification of the information to be protected, which are based on risk, practicality and other considerations.

Our customers, colleagues, and others rely on us to protect their information. A data security breach could severely damage our credibility, cause loss of business and other harm to affected individuals. Strong data security requires diligence by all colleagues, contractors, and any others accessing or using our data assets. Data Protection is part of everyone's job.

Guiding Principles

All colleagues should keep in mind the following principles for data protection:

- i. Energizer protects the confidentiality, integrity and access to its data assets.
- ii. Energizer will comply with applicable data privacy and data protection laws.
- iii. Energizer balances the needs for business efficiency with the need to protect personal, proprietary and other confidential information from unnecessary risk.
- iv. Energizer only grants access to personal, proprietary and other confidential information to those with a need to know and who are obligated to maintain the security of the information.
- v. Energizer colleagues are the first and best line of defense against data security incidents, and it is every colleague's responsibility to uphold the practices of this Policy.
- vi. Energizer's network, systems and other assets are primarily for business purposes. Except where applicable law provides otherwise, you should have no expectation of privacy when using Energizer's network or systems, including, but not limited to, transmitting and storing files, data, and messages.

Section 2: Policy Owner and Statement of Responsibility

This policy is owned by the Associate General Counsel, Global Ethics & Compliance. It is the responsibility of this individual, along with Legal, to implement, review annually, and revise this policy as needed.

Name	Title	Phone	Email
Karen Benson	Associate General Counsel, Global Ethics & Compliance	954.593.6876	karen.benson@energizer.com



Global Data Protection Policy

Effective Date: February 2018

Last Revision: April 2025

Section 3: Protecting Personal Data

3.1 Collection & Processing of Colleague Data

In order to effectively run its business, Energizer needs to collect and use certain personal information about our colleagues. Global data privacy laws and regulations require appropriate collection, storage, processing, sharing, transfer and use of personal data, including the personal data of colleagues ("Colleague Personal Data"). It is the fundamental responsibility of colleagues, as outlined in the Code of Conduct, to use the data only for the purpose it was intended and to appropriately protect this data.

Certain data, including sensitive personal data and personal data, is collected from colleagues -- and in some instances candidates for employment -- either by the company or company's authorized third parties to administer all aspects of employment, including but not limited to: payroll, compensation, travel, expense reimbursement, online giving, benefits administration, disciplinary and grievance procedures, time & attendance, training course management, and career management.

When necessary for business purposes, and allowed by law, Energizer may also access and store emails and documents, including resumes (CVs), that may contain personal or sensitive data. Energizer may also collect colleague data when it monitors communications and systems to protect the business against viruses and malware or to ensure compliance with policies, laws and regulations.

3.2 Types of Colleague Data Collected

3.2(a) – Personal Data

In the European Union (EU) and many other countries, "personal data" is broadly defined as any information relating to an identified or identifiable person (i.e., a person who can be identified directly or indirectly by reference to a name, ID number, etc.). Simply put, personal data can include a person's name, email address, physical address, or the like.

3.2(b) – Sensitive Personal Data

Data privacy laws vary by country and some data elements are considered sensitive in certain jurisdictions and require additional protection because inappropriate use of this data can lead to identity theft. For example, Sensitive Personal Data may include:

- Bank account or credit card information (such as account number and routing number)
- National ID, such as Social Security Number
- Passport #
- Salary & related compensation information
- Biometric, health and medical information



Global Data Protection Policy

Effective Date: February 2018

Last Revision: April 2025

- Racial or ethnic origin
- Political or religious beliefs
- Union memberships

3.3 Data Protection Laws

Many countries have promulgated data privacy laws that specify requirements for the “processing” of personal data. “Processing” can include actions such as collecting, using, storing, altering, disclosing, or transmitting personal data, among others. For example, processing of personal data of EU citizens (including colleagues & applicants) is regulated such that any data collection, processing, or transfer outside of the EU (or other approved states) must comply with the laws, such as the EU’s General Data Protection Regulations (GDPR).

Any transfer of EU personal data outside of the EU --which includes accessing the EU personal data from outside the EU-- requires appropriate safeguards prior to the data transfer. Additionally, sharing EU personal data with a third party (even those we have a contract with) outside of the EU requires appropriate security and should be coordinated with Legal and the Head of Ethics & Compliance.

3.4 – Your Responsibilities to Protect Colleague Data

Colleagues and contractors are obligated to comply with all aspects of this Policy that apply to them. If you have access to Personal Data and/or Sensitive Personal Data, or other individual’s data based on your role within the Company, it is your duty to implement Energizer approved controls to secure and protect that data and limit access to the data to only those with a need to know and only for necessary and legitimate business purposes.

Energizer sets forth the following guidelines for Colleagues who are accessing, saving and/or transmitting (i.e., processing) files with Personal Data or Sensitive Personal Data:

- i. Conspicuously mark all documents, files or emails that contain Sensitive Personal Data with the following marking:

“Personal and Confidential”

- ii. Files containing this type of data should only be saved in a secure location such as OneDrive, but may be stored **temporarily** on secured company resources such as laptop or desktop computers, eventually being stored in OneDrive.
- iii. Protect Sensitive Personal Data files with encryption and/or passwords. Sensitive Personal Data files should only be transmitted using secure/encrypted methods, such as Subject Line Encryption, Citrix ShareFile or secure transmission portals with a vendor.
- iv. Before sharing EU Personal Data and Sensitive Personal Data with third parties, ensure that it is both appropriate and necessary and contact the Privacy resources below to ensure appropriate safeguards are in place.



Global Data Protection Policy

Effective Date: February 2018

Last Revision: April 2025

-
- v. Remember to lock your computer if you need to step away from it.
 - vi. Do not leave your laptop in plain sight, or unsecured, in your car or a hotel room and do not walk away from it at a public location such as an airport.
 - vii. Be aware that even data such as names, email addresses, and other information that relates to an identified or identifiable person may be considered "Personal Data" under many countries' privacy laws and may require additional protections.
 - viii. Data should be deleted from your computer as soon as you no longer have a need to access it, unless subject to litigation hold or other records retention schedule.

Finally, notify the Head of Ethics & Compliance if you are unsure if certain information or files can be shared with another party, if you become aware of sensitive information that was shared by mistake, or unauthorized, or if your laptop or mobile device (phone or tablet) was lost, stolen or compromised. Stolen laptops or mobile devices should also be reported to IT Concierge.

Section 4: Protecting Company Confidential or Proprietary Data

Energizer Confidential Data

Confidential Information is information that may cause harm to Energizer, its customers, colleagues, or other entities or individuals if improperly disclosed, or information that is not otherwise publicly available. Harms may relate to an individual's privacy, Energizer's strategic business position or that of its customers, or legal or regulatory liabilities. In accordance with your roles and responsibilities, you may have access to Energizer Confidential Data.

Examples of Confidential Data include strategic plans, marketing plans, financial data, customer lists, contracts, business plans, unpublished patents, trade secrets, M&A documentation, information subject to a non-disclosure agreement, or other technical or business information.

This Policy requires protecting Confidential Data in the storage, dissemination and sharing both inside and outside the company using appropriate administrative, physical, and technical safeguards according to the risks posed by the possible unauthorized access to the data.

4.1 Your Responsibilities to Protect Company Data

Unless it is marked otherwise or clearly intended to be Public Information, treat all information/data as if it Energizer Confidential Data, regardless of its source or form, including electronic, paper, verbal, or other information.

Energizer sets forth the following guidelines for accessing, saving and/or transmitting (i.e., processing) files containing Energizer Confidential Data:

- Conspicuously mark all documents, files or emails that contain Energizer Confidential Data with the following:



Global Data Protection Policy

Effective Date: February 2018

Last Revision: April 2025

“Energizer Proprietary and Confidential”

- Files containing this type of data should only be saved in a secure location such as OneDrive, but may be stored temporarily on secured company resources such as laptop or desktop computers, eventually being stored in OneDrive.
- Protect Confidential Data with appropriate encryption and/or passwords and only transmit using secure methods, such as Subject Line Encryption, Citrix ShareFile or secure transmission portals.
- Remember to lock your computer if you need to step away from it.
- Do not leave your laptop in plain sight, or unsecured, in your car or a hotel room and do not walk away from it at a public location such as an airport.
- Confidential Data should be deleted from your computer as soon as you no longer have a need to access it, unless subject to litigation hold or other to comply with Energizer’s Records Retention schedule.
- Only discuss Confidential Data in non-public places or by taking reasonable steps to avoid being heard.
- Only scan, distribute, copy and distribute Confidential Data to the extent necessary, and ensure the receiving party is subject to a non-disclosure agreement or under similar obligations of confidentiality.

Return all Confidential Data in your possession at the end of your employment and remember that your obligation to protect confidential data survives past the termination of employment. **If you become aware that Confidential Data was shared with unauthorized parties (intentionally or unintentionally), or your laptop or mobile device was lost, stolen or compromised and it contained Confidential Data, please contact the Head of Ethics & Compliance and IT Concierge immediately to report the incident.**

Have a question or a concern?

There are many ways to ask a question or raise a concern regarding this policy. Choose the option you are most comfortable using. Whichever option you choose, your confidentiality will be respected, and retaliation will not be tolerated:

- Your manager or next level leadership
- Human Resources
- Ethics & Compliance energizercompliance@energizer.com
- Legal
- Energizer HelpLine: www.EnergizerHelpLine.com
 - Call 1-877-521-5625 (U.S.)
 - Additional phone numbers at www.EnergizerHelpLine.com
 - Text “Report” to 314-668-1383 (North America only)
 - you can remain anonymous if you choose
 - available 24 hours and operated by a 3rd party provider



Global Data Protection Policy

Effective Date: February 2018

Last Revision: April 2025

Section 5: Related Policies and Standards

Policy Name
Code of Conduct
Information Technology Acceptable Use Policy
Records and Information Management (RIM) Policy

Section 6: Revision History

The policy owner will review and update this policy as necessary at least once every fiscal year.

Revision Number	Effective Date	Owner	Description of Change
4	April 2024	Seth Smoker	Updated Policy Owner; changed “head of ethics & compliance” to “Associate General Counsel, Global Ethics & Compliance” and changed contact information to Karen Benson
3	March 2021	Ronnie Kann	Updated contact information for Energizer HelpLine
2	November 2020	Ronnie Kann	Updated policy owner; changed “chief compliance officer” to “head of ethics & compliance”; added how to ask a question or raise a concern; add RIM policy and Code of Conduct to related policy and standards
1	January 2018	Kathy Rehmer	New policy

Section 7: Required Approval

Signature on File _____

Signature on File _____

Section 1: الغرض من هذه السياسة

تعزز سياسة حماية البيانات العالمية هذه ("السياسة") التوازن الفعال بين ممارسات أمن المعلومات واحتياجات العمل، مع الحفاظ على الامتثال للقوانين ذات الصلة. تساعد هذه السياسة Energizer على الوفاء بالتزاماتنا القانونية مع الحفاظ على قدرة الشركة على أن تكون مرنة وتلبي توقعات العملاء. كما هو موضح أدناه بمزيد من التفصيل، تتطلب Energizer مستويات مختلفة من الضوابط الأمنية اعتماداً على تصنيف المعلومات المراد حمايتها، والتي تستند إلى المخاطر والعملية واعتبارات أخرى.

يعتمد عملاؤنا وزملاؤنا وغيرهم علينا لحماية معلوماتهم. قد يؤدي خرق أمن البيانات إلى إلحاق ضرر شديد بمصداقيتنا، ويتسبب في خسارة الأعمال التجارية وغيرها من الأضرار للأفراد المتضررين. يتطلب أمن البيانات القوي بذل العناية الواجبة من قبل جميع الزملاء والمتعاقدين وأي آخرين يمكنهم الوصول إلى أصول البيانات الخاصة بنا أو استخدامها. إن حماية البيانات جزء من مهمة الجميع.

المبادئ التوجيهية

ينبغي على جميع الزملاء مراعاة المبادئ التالية لحماية البيانات:

- i. تحمي Energizer السرية والنزاهة والوصول إلى أصول البيانات الخاصة بها.
- ii. سنتوافق مع Energizer مع قوانين خصوصية البيانات وحماية البيانات المعمول بها.
- iii. توازن Energizer بين احتياجات كفاءة العمل والحاجة إلى حماية المعلومات الشخصية والخاصة وغيرها من المعلومات السرية من المخاطر غير الضرورية.
- iv. تمنح Energizer حق الوصول إلى المعلومات الشخصية والملكية وغيرها من المعلومات السرية فقط لأولئك الذين يحتاجون إلى معرفتها والذين يلتزمون بالحفاظ على أمن المعلومات.
- v. يعد زملاء Energizer خط الدفاع الأول والأفضل ضد حوادث أمن البيانات، وتقع على عاتق كل زميل مسؤولية الالتزام بممارسات هذه السياسة.
- vi. إن شبكة Energizer وأنظمتها وأصولها الأخرى مخصصة في المقام الأول لأغراض تجارية. باستثناء الحالات التي ينص فيها القانون المعمول به على خلاف ذلك، يجب ألا تتوقع أي خصوصية عند استخدام شبكة Energizer أو أنظمتها، بما في ذلك على سبيل المثال لا الحصر، نقل وتخزين الملفات والبيانات والرسائل.

Section 2: مالك السياسة وبيان المسؤولية

هذه السياسة مملوكة للمستشار العام المساعد، المكتب العالمي للأخلاقيات والامتثال. تقع على عاتق هذا الشخص، إلى جانب القسم القانوني، مسؤولية تنفيذ هذه السياسة ومراجعتها سنوياً وتنقيحها حسب الحاجة.

الاسم	العنوان	الهاتف	البريد الإلكتروني
كارين بنسون	المستشار العام المساعد، المكتب العالمي للأخلاقيات والامتثال	954.593.6876	karen.benson@energizer.com

Section 3: حماية البيانات الشخصية

3.1 جمع بيانات الزملاء ومعالجتها

لإدارة أعمالها بفعالية، تحتاج Energizer إلى جمع معلومات شخصية معينة عن زملائنا واستخدامها. تتطلب قوانين ولوائح خصوصية البيانات العالمية جمع البيانات الشخصية وتخزينها ومعالجتها ومشاركتها ونقلها واستخدامها بشكل مناسب، بما في ذلك البيانات الشخصية للزملاء ("البيانات الشخصية للزميل"). يتحمل الزملاء المسؤولية الأساسية، كما هو موضح في مدونة قواعد السلوك، عن استخدام البيانات للغرض المقصود منها فقط وحماية هذه البيانات بشكل مناسب.

يتم جمع بعض البيانات، بما في ذلك البيانات الشخصية الحساسة والبيانات الشخصية، من الزملاء - وفي بعض الحالات المرشحين للعمل - إما من قبل الشركة أو الجهات الخارجية المصرح لها بإدارة جميع جوانب التوظيف، بما في ذلك على سبيل المثال لا الحصر: الرواتب، والتعويضات، والسفر، وتسديد النفقات، والعطاء عبر الإنترنت، إدارة الفوائد والإجراءات التأديبية وإجراءات التظلم والوقت والحضور وإدارة الدورات التدريبية والإدارة المهنية.

عند الضرورة لأغراض تجارية، ويسمح القانون بذلك، يجوز لشركة Energizer أيضا الوصول إلى رسائل البريد الإلكتروني والمستندات وتخزينها، بما في ذلك السير الذاتية (CVs)، التي قد تحتوي على بيانات شخصية أو حساسة. قد تجمع Energizer أيضا بيانات الزملاء عندما تراقب الاتصالات والأنظمة لحماية الشركة من الفيروسات والبرامج الضارة أو لضمان الامتثال للسياسات والقوانين واللوائح.

3.2 أنواع بيانات الزملاء التي تم جمعها

3.2(a) البيانات الشخصية

في الاتحاد الأوروبي (EU) والعديد من البلدان الأخرى، تعرف "البيانات الشخصية" على نطاق واسع بأنها أي معلومات تتعلق بشخص محدد الهوية أو يمكن التعرف عليه (أي شخص يمكن التعرف عليه بشكل مباشر أو غير مباشر بالرجوع إلى اسم أو رقم هوية، وما إلى ذلك). ببساطة، يمكن أن تتضمن البيانات الشخصية اسم الشخص أو عنوان بريده الإلكتروني أو عنوانه الفعلي أو ما شابه ذلك.

3.2(b) البيانات الشخصية الحساسة

تختلف قوانين خصوصية البيانات حسب البلد وتعتبر بعض عناصر البيانات حساسة في بعض الولايات القضائية وتتطلب حماية إضافية لأن الاستخدام غير الملائم لهذه البيانات قد يؤدي إلى سرقة الهوية. على سبيل المثال، قد تتضمن البيانات الشخصية الحساسة ما يلي:

- معلومات الحساب المصرفي أو بطاقة الائتمان (مثل رقم الحساب ورقم التوجيه)
- الهوية الوطنية، مثل رقم الضمان الاجتماعي
- رقم جواز السفر
- معلومات الراتب والتعويضات ذات الصلة
- المعلومات البيومترية والصحية والطبية
- الأصل العرقي أو العرقي
- المعتقدات السياسية أو الدينية
- عضوية النقابات

3.3 قوانين حماية البيانات

أصدرت العديد من البلدان قوانين خصوصية البيانات التي تحدد متطلبات "معالجة" البيانات الشخصية. يمكن أن تتضمن "المعالجة" إجراءات مثل التجميع أو الاستخدام أو التخزين أو التغيير أو الكشف أو نقل البيانات الشخصية، من بين أمور أخرى. على سبيل المثال، يتم تنظيم معالجة البيانات الشخصية لمواطني الاتحاد الأوروبي (بما في ذلك الزملاء ومقدمي الطلبات) بحيث يجب أن يتوافق أي جمع للبيانات أو معالجتها أو نقلها خارج الاتحاد الأوروبي (أو أي دولة أخرى معتمدة) مع القوانين، مثل اللوائح العامة لحماية البيانات في الاتحاد الأوروبي (GDPR).

يتطلب أي نقل للبيانات الشخصية للاتحاد الأوروبي خارج الاتحاد الأوروبي - بما في ذلك الوصول إلى البيانات الشخصية للاتحاد الأوروبي من خارج الاتحاد الأوروبي - ضمانات مناسبة قبل نقل البيانات. بالإضافة إلى ذلك، تتطلب مشاركة البيانات الشخصية للاتحاد الأوروبي مع طرف ثالث (حتى أولئك الذين أبرمنا عقدا معهم) خارج الاتحاد الأوروبي توفير الأمن المناسب وينبغي تنسيقها مع قسم الشؤون القانونية ورئيس قسم الأخلاقيات والامتثال.

3.4 مسؤولياتك لحماية بيانات الزملاء

يلتزم الزملاء والمقاولون بالامتثال لجميع جوانب هذه السياسة التي تنطبق عليهم. إذا كان لديك حق الوصول إلى البيانات الشخصية و/أو البيانات الشخصية الحساسة، أو بيانات شخص آخر استنادا إلى دورك داخل الشركة، فمن واجبك تنفيذ الضوابط المعتمدة من Energizer لتأمين وحماية تلك البيانات وتقييد الوصول إلى البيانات فقط لأولئك الذين يحتاجون إلى المعرفة فقط لأغراض العمل الضرورية والمشروعة.

تحدد Energizer الإرشادات التالية للزملاء الذين يقومون بالوصول إلى الملفات و/أو حفظها و/أو إرسالها (أي معالجتها) باستخدام البيانات الشخصية أو البيانات الشخصية الحساسة:

i. ضع علامة واضحة على جميع المستندات أو الملفات أو رسائل البريد الإلكتروني التي تحتوي على بيانات شخصية حساسة بالعلامة التالية:

"شخصي وسري"

- ii. يجب حفظ الملفات التي تحتوي على هذا النوع من البيانات في موقع آمن فقط مثل OneDrive، ولكن يمكن تخزينها مؤقتا على موارد الشركة الآمنة مثل أجهزة الكمبيوتر المحمولة أو أجهزة الكمبيوتر المكتبية، ويتم تخزينها في النهاية في OneDrive.
- iii. حماية ملفات البيانات الشخصية الحساسة باستخدام التشفير و/أو كلمات المرور. يجب نقل ملفات البيانات الشخصية الحساسة فقط باستخدام طرق آمنة/مشفرة، مثل تشفير سطر الموضوع أو Citrix ShareFile أو بوابات الإرسال الآمنة مع أحد الموردين.
- iv. قبل مشاركة بيانات الاتحاد الأوروبي الشخصية والبيانات الشخصية الحساسة مع أطراف ثالثة، تأكد من أنها مناسبة وضرورية على حد سواء واتصل بموارد الخصوصية أدناه لضمان وجود الضمانات المناسبة.
- v. تذكر تأمين الكمبيوتر إذا كنت بحاجة إلى الابتعاد عنه.
- vi. لا تترك الكمبيوتر المحمول على مرأى من الجميع أو في مكان غير آمن في سيارتك أو في غرفة فندق ولا تمشي بعيدا عنه في مكان عام مثل المطار.
- vii. انتبه إلى أنه حتى البيانات مثل الأسماء وعناوين البريد الإلكتروني والمعلومات الأخرى المتعلقة بشخص محدد أو يمكن التعرف عليه يمكن اعتبارها "بيانات شخصية" بموجب قوانين الخصوصية في العديد من البلدان وقد تتطلب حماية إضافية.
- viii. يجب حذف البيانات من الكمبيوتر بمجرد عدم الحاجة إلى الوصول إليها، إلا إذا كانت خاضعة لاحتجاز دعوى قضائية أو جدول استبقاء سجلات آخر.

وأخيرا، أبلغ رئيس قسم الأخلاقيات والامتثال إذا لم تكن متأكدا مما إذا كان من الممكن مشاركة معلومات أو ملفات معينة مع طرف آخر، أو إذا علمت بمعلومات حساسة تمت مشاركتها عن طريق الخطأ، أو غير مصرح بها، أو إذا فقد الكمبيوتر المحمول أو الجهاز المحمول (الهاتف أو الكمبيوتر اللوحي) أو سرق أو تعرض للاختراق. يجب أيضا إبلاغ مسؤول قسم تكنولوجيا المعلومات عن أجهزة الكمبيوتر المحمول أو الأجهزة المحمولة المسروقة.

Section 4: حماية بيانات الشركة السرية أو الملكية

بيانات Energizer السرية

المعلومات السرية هي المعلومات التي قد تلحق الضرر بشركة Energizer أو عملائها أو زملائها أو الكيانات أو الأفراد الآخرين إذا تم الكشف عنها بشكل غير صحيح، أو المعلومات التي لا تكون متاحة للجمهور بخلاف ذلك. قد تتعلق الأضرار بخصوصية الفرد، أو الموقف التجاري الاستراتيجي لشركة Energizer أو موقف عملائها، أو المسؤوليات القانونية أو التنظيمية. وفقا لأدوارك ومسؤولياتك، قد تتمكن من الوصول إلى بيانات Energizer السرية.

تتضمن أمثلة البيانات السرية الخطط الاستراتيجية وخطط التسويق والبيانات المالية وقوائم العملاء والعقود خطط العمل، أو براءات الاختراع غير المنشورة، أو الأسرار التجارية، أو وثائق الاندماج والاستحواذ، أو المعلومات الخاضعة لاتفاقية عدم الإفصاح، أو غيرها من المعلومات الفنية أو التجارية.

تتطلب هذه السياسة حماية البيانات السرية في التخزين والنشر والمشاركة داخل الشركة وخارجها باستخدام وسائل حماية إدارية ومادية وتقنية مناسبة وفقا للمخاطر التي يفرضها الوصول غير المصرح به المحتمل إلى البيانات.

4.1 مسؤولياتك لحماية بيانات الشركة

تتعامل مع جميع المعلومات/البيانات كما لو أنها بيانات سرية، بغض النظر عن مصدرها أو شكلها، بما في ذلك المعلومات الإلكترونية أو الورقية أو اللفظية أو غيرها، ما لم يتم وضع علامة بخلاف ذلك أو المقصود منها بوضوح أن تكون معلومات عامة.

تحدد Energizer الإرشادات التالية للوصول إلى الملفات التي تحتوي على بيانات Energizer السرية وحفظها و/أو إرسالها (أي معالجتها):

- ضع علامة واضحة على كل المستندات أو الملفات أو رسائل البريد الإلكتروني التي تحتوي على بيانات Energizer السرية بما يلي:

"ملكية الطاقة وسرية"

- يجب حفظ الملفات التي تحتوي على هذا النوع من البيانات في موقع آمن فقط مثل OneDrive، ولكن يمكن تخزينها مؤقتاً على موارد الشركة الأمانة مثل أجهزة الكمبيوتر المحمولة أو أجهزة الكمبيوتر المكتبية، ويتم تخزينها في النهاية في OneDrive.
- قم بحماية البيانات السرية باستخدام تشفير و/أو كلمات مرور مناسبة وقم فقط بالنقل باستخدام طرق آمنة، مثل تشفير سطر الموضوع أو Citrix ShareFile أو بوابات الإرسال الآمنة.
- تذكر تأمين الكمبيوتر إذا كنت بحاجة إلى الابتعاد عنه.
- لا تترك الكمبيوتر المحمول على مرأى من الجميع أو في مكان غير آمن في سيارتك أو في غرفة فندق ولا تمشي بعيداً عنه في مكان عام مثل المطار.
- يجب حذف البيانات السرية من الكمبيوتر الخاص بك بمجرد عدم الحاجة إلى الوصول إليها، ما لم تكن عرضة لاحتجاز دعوى قضائية أو أي إجراء آخر للامتثال لجدول الاحتفاظ بالسجلات الخاص بشركة Energizer.
- ناقش البيانات السرية فقط في الأماكن غير العامة أو من خلال اتخاذ خطوات معقولة لتجنب سماعها.
- مسح البيانات السرية وتوزيعها ونسخها وتوزيعها فقط بالقدر الضروري، والتأكد من خضوع الطرف المتلقي لاتفاقية عدم الإفصاح أو بموجب التزامات مماثلة تتعلق بالسرية.

أعد جميع البيانات السرية التي بحوزتك في نهاية عملك وتذكر أن التزامك بحماية البيانات السرية يظل قائماً بعد انتهاء العمل. إذا علمت أنه تمت مشاركة البيانات السرية مع أطراف غير مصرح لها (عمداً أو عن غير قصد)، أو أن الكمبيوتر المحمول أو الجهاز المحمول الخاص بك قد فقد أو سرق أو تعرض للخطر وكان يحتوي على بيانات سرية، فيرجى الاتصال برئيس قسم الأخلاقيات والامتثال وبواب قسم تكنولوجيا المعلومات على الفور للإبلاغ عن الحادث.

هل لديك سؤال أو مخاوف؟

هناك العديد من الطرق لطرح سؤال أو الإبلاغ عن مخاوف تتعلق بهذه السياسة. اختر الخيار الذي تشعر براحة أكبر عند استخدامه. أيا كان الخيار الذي تختاره، سيتم احترام السرية الخاصة بك ولن يتم التسامح مع الانتقام:

- مديرك أو قيادتك من المستوى التالي
- الموارد البشرية
- الأخلاقيات والامتثال energizercompliance@energizer.com
- الشؤون القانونية
- خط مساعدة Energizer: www.EnergizerHelpLine.com
- اتصل بالرقم 1-877-521-5625 (الولايات المتحدة)
- أرقام هواتف إضافية على www.EnergizerHelpLine.com
- نص "Report" (تقرير) إلى 1383-668-314 (أمريكا الشمالية فقط)
- يمكنك أن تظل مجهول الهوية إذا اخترت ذلك
- متوفر على مدار 24 ساعة ويتم تشغيله من قبل 3 موفر خدمة تابع لجهة خارجية

Section 5: السياسات والمعايير ذات الصلة

اسم السياسة
مدونة قواعد السلوك سياسة الاستخدام المقبول لتكنولوجيا المعلومات نهج إدارة السجلات والمعلومات (RIM)

Section 6: البيانات التاريخية للمراجعة

سيقوم مالك السياسة بمراجعة هذه السياسة وتحديثها حسب الضرورة مرة واحدة على الأقل كل سنة مالية.

رقم المراجعة	تاريخ السريان	المالك	وصف التغيير
4	أبريل 2024	سيث سموكر	مالك السياسة المحدث؛ غير "رئيس قسم الأخلاقيات والامتثال" إلى "مستشار عام مساعد، المكتب العالمي للأخلاقيات والامتثال" وغير معلومات الاتصال إلى كارين بنسون
3	مارس 2021	روني كان	معلومات الاتصال المحدثة لخط المساعدة Energizer
2	نوفمبر 2020	روني كان	تحديث مالك السياسة؛ تغيير "كبير مسؤولي الامتثال" إلى "رئيس الأخلاقيات والامتثال"؛ إضافة كيفية طرح سؤال أو الإبلاغ عن مخاوف؛ إضافة سياسة إدارة المخاطر ومدونة قواعد السلوك إلى السياسات والمعايير ذات الصلة
1	يناير 2018	كاثي ريمر	سياسة جديدة

Section 7: الموافقة المطلوبة

التوقيع على الملف _____
التوقيع على الملف _____

Kebijakan Perlindungan data Global

Tanggal efektif: 2018 Februari

Revisi terakhir: April 2025

Section 1: Tujuan dari kebijakan ini

Kebijakan Perlindungan data Global ini (“Kebijakan”) mempromosikan keseimbangan yang efektif antara praktik keamanan informasi dan kebutuhan bisnis, sambil tetap mematuhi undang-undang yang relevan. Kebijakan ini membantu Energizer memenuhi kewajiban hukum kami sambil mempertahankan kemampuan bisnis untuk menjadi gesit dan memenuhi harapan pelanggan. Seperti yang dijelaskan di bawah ini secara lebih rinci, Energizer membutuhkan tingkat kontrol keamanan yang berbeda tergantung pada klasifikasi informasi yang akan dilindungi, yang didasarkan pada risiko, kepraktisan, dan pertimbangan lainnya.

Pelanggan, kolega, dan orang lain bergantung pada kami untuk melindungi informasi mereka. Pelanggaran keamanan data dapat sangat merusak kredibilitas kami, menyebabkan hilangnya bisnis dan bahaya lainnya bagi individu yang terkena dampak. Keamanan data yang kuat memerlukan ketekunan oleh semua kolega, kontraktor, dan pihak lain yang mengakses atau menggunakan aset data kami. Perlindungan data adalah bagian dari pekerjaan setiap orang.

Prinsip-prinsip bimbingan

Semua kolega harus mengingat prinsip-prinsip berikut untuk perlindungan data:

- i. Energizer melindungi kerahasiaan, integritas, dan akses ke aset datanya.
- ii. Energizer akan mematuhi undang-undang privasi data dan perlindungan data yang berlaku.
- iii. Energizer menyeimbangkan kebutuhan untuk efisiensi bisnis dengan kebutuhan untuk melindungi informasi pribadi, kepemilikan dan rahasia lainnya dari risiko yang tidak perlu.
- iv. Energizer hanya memberikan akses ke informasi pribadi, hak milik, dan informasi rahasia lainnya kepada mereka yang perlu mengetahui dan yang berkewajiban untuk menjaga keamanan informasi.
- v. Rekan Energizer adalah garis pertahanan pertama dan terbaik terhadap insiden keamanan data, dan merupakan tanggung jawab setiap kolega untuk menegakkan praktik Kebijakan ini.
- vi. Jaringan, sistem, dan aset Energizer lainnya terutama untuk tujuan bisnis. Kecuali jika hukum yang berlaku menyatakan sebaliknya, Anda tidak boleh mengharapkan privasi saat menggunakan jaringan atau sistem Energizer, termasuk, namun tidak terbatas pada, mentransmisikan dan menyimpan file, data, dan pesan.

Section 2: Pemilik kebijakan dan pernyataan tanggung jawab

Kebijakan ini dimiliki oleh Associate General Counsel, Global Ethics & Compliance. Adalah tanggung jawab individu ini, bersama dengan hukum, untuk menerapkan, meninjau setiap tahun, dan merevisi kebijakan ini sesuai kebutuhan.

Nama	Judul	Telepon	Email
Karen Benson	Associate General Counsel, Etika & Kepatuhan Global	954.593.6876	karen.benson@energizer.com

Section 3: Melindungi data pribadi**3.1 Pengumpulan & pemrosesan data kolega**

Agar dapat menjalankan bisnisnya secara efektif, Energizer perlu mengumpulkan dan menggunakan informasi pribadi tertentu tentang kolega kami. Undang-undang dan peraturan privasi data global memerlukan pengumpulan, penyimpanan, pemrosesan, pembagian, transfer, dan penggunaan data pribadi yang sesuai, termasuk data pribadi kolega ("data pribadi kolega"). Merupakan tanggung jawab mendasar kolega, sebagaimana diuraikan dalam Pedoman perilaku, untuk menggunakan data hanya untuk tujuan yang dimaksudkan dan untuk melindungi data ini dengan tepat.

Data tertentu, termasuk data pribadi sensitif dan data pribadi, dikumpulkan dari rekan kerja - dan dalam beberapa kasus kandidat untuk pekerjaan - baik oleh perusahaan atau pihak ketiga resmi perusahaan untuk mengelola semua aspek pekerjaan, termasuk namun tidak terbatas pada: Penggajian, kompensasi, perjalanan, penggantian biaya, pemberian online, manfaat administrasi, disiplin dan keluhan prosedur, waktu & kehadiran, pelatihan manajemen kursus, dan manajemen karir.

Bila diperlukan untuk tujuan bisnis, dan diizinkan oleh hukum, Energizer juga dapat mengakses dan menyimpan email dan dokumen, termasuk resume (CV), yang mungkin berisi data pribadi atau sensitif. Energizer juga dapat mengumpulkan data kolega ketika memantau komunikasi dan sistem untuk melindungi bisnis dari virus dan malware atau untuk memastikan kepatuhan terhadap kebijakan, hukum, dan peraturan.

3.2 Jenis data kolega yang dikumpulkan**3.2(a) Data pribadi**

Di Uni Eropa (UE) dan banyak negara lain, "data pribadi" secara luas didefinisikan sebagai informasi apa pun yang berkaitan dengan orang yang diidentifikasi atau diidentifikasi (yaitu, orang yang dapat diidentifikasi secara langsung atau tidak langsung dengan mengacu pada nama, nomor ID, dll.). Sederhananya, data pribadi dapat mencakup nama seseorang, alamat email, alamat fisik, atau sejenisnya.

3.2(b) Data pribadi yang sensitif

Undang-undang privasi data bervariasi menurut negara dan beberapa elemen data dianggap sensitif di yurisdiksi tertentu dan memerlukan perlindungan tambahan karena penggunaan data

ini yang tidak tepat dapat menyebabkan pencurian identitas. Misalnya, data pribadi yang sensitif dapat mencakup:

- Rekening bank atau informasi kartu kredit (seperti nomor rekening dan nomor routing)
- ID Nasional, seperti nomor Jaminan sosial
- Paspor #
- Informasi gaji & kompensasi terkait
- Informasi biometrik, kesehatan dan medis
- Asal ras atau etnis
- Keyakinan politik atau agama
- Keanggotaan Union

3.3 Undang-undang Perlindungan data

Banyak negara telah mengumumkan undang-undang privasi data yang menentukan persyaratan untuk “pemrosesan” data pribadi. “Pemrosesan” dapat mencakup tindakan seperti mengumpulkan, menggunakan, menyimpan, mengubah, mengungkapkan, atau mengirimkan data pribadi, antara lain. Misalnya, pemrosesan data pribadi warga negara UE (termasuk kolega & pelamar) diatur sedemikian rupa sehingga setiap pengumpulan, pemrosesan, atau transfer data di luar UE (atau negara lain yang disetujui) harus mematuhi undang-undang, seperti Peraturan Perlindungan data umum UE (GDPR).

Setiap transfer data pribadi Uni Eropa di luar UE - yang mencakup mengakses data pribadi UE dari luar UE - memerlukan perlindungan yang tepat sebelum transfer data. Selain itu, berbagi data pribadi UE dengan pihak ketiga (bahkan yang memiliki kontrak dengan kami) di luar UE memerlukan keamanan yang sesuai dan harus dikoordinasikan dengan legal dan Kepala Etika & Kepatuhan.

3.4 Tanggung jawab Anda untuk melindungi data kolega

Kolega dan kontraktor diwajibkan untuk mematuhi semua aspek Kebijakan ini yang berlaku bagi mereka. Jika Anda memiliki akses ke data pribadi dan/atau data pribadi yang sensitif, atau data individu lain berdasarkan peran Anda dalam perusahaan, adalah tugas Anda untuk menerapkan kontrol yang disetujui Energizer untuk mengamankan dan melindungi data tersebut dan membatasi akses ke data hanya kepada mereka yang perlu mengetahui dan hanya untuk tujuan bisnis yang diperlukan dan sah.

Energizer menetapkan pedoman berikut untuk kolega yang mengakses, menyimpan, dan/atau mentransmisikan (yaitu, memproses) file dengan data pribadi atau data pribadi sensitif:

- i. Secara mencolok menandai semua dokumen, file, atau email yang berisi data pribadi sensitif dengan tanda berikut:

“Pribadi dan rahasia”

Kebijakan Perlindungan data Global

Tanggal efektif: 2018 Februari

Revisi terakhir: April 2025

-
- ii. File yang berisi jenis data ini hanya boleh disimpan di lokasi yang aman seperti OneDrive, tetapi dapat disimpan **sementara** di sumber daya perusahaan yang aman seperti komputer laptop atau desktop, yang akhirnya disimpan di OneDrive.
 - iii. Lindungi file data pribadi sensitif dengan enkripsi dan/atau kata sandi. File data pribadi sensitif hanya boleh ditransmisikan menggunakan metode aman/terenkripsi, seperti enkripsi baris subjek, Citrix ShareFile, atau portal transmisi aman dengan vendor.
 - iv. Sebelum berbagi data pribadi UE dan data pribadi sensitif dengan pihak ketiga, pastikan bahwa data tersebut sesuai dan perlu dan hubungi sumber daya Privasi di bawah ini untuk memastikan perlindungan yang tepat telah diterapkan.
 - v. Ingatlah untuk mengunci komputer Anda jika Anda perlu menjauh darinya.
 - vi. Jangan meninggalkan laptop Anda di depan mata, atau tanpa jaminan, di mobil Anda atau kamar hotel dan jangan berjalan menjauh dari itu di lokasi umum seperti bandara.
 - vii. Perlu diketahui bahwa bahkan data seperti nama, alamat email, dan informasi lain yang berkaitan dengan orang yang diidentifikasi atau diidentifikasi dapat dianggap sebagai “data pribadi” di bawah undang-undang privasi banyak negara dan mungkin memerlukan perlindungan tambahan.
 - viii. Data harus dihapus dari komputer Anda segera setelah Anda tidak lagi memiliki kebutuhan untuk mengaksesnya, kecuali tunduk pada penangguhan litigasi atau jadwal penyimpanan catatan lainnya.

Terakhir, beri tahu Kepala Etika & Kepatuhan jika Anda tidak yakin apakah informasi atau file tertentu dapat dibagikan dengan pihak lain, jika Anda mengetahui informasi sensitif yang dibagikan secara tidak sengaja, atau tidak sah, atau jika laptop atau perangkat seluler Anda (telepon atau tablet) hilang, dicuri, atau dikompromikan. Laptop atau perangkat seluler yang dicuri juga harus dilaporkan ke IT Concierge.

Section 4: Melindungi data rahasia atau kepemilikan perusahaan

Data rahasia Energizer

Informasi rahasia adalah informasi yang dapat menyebabkan kerusakan pada Energizer, pelanggan, kolega, atau entitas atau individu lain jika diungkapkan secara tidak benar, atau informasi yang tidak tersedia untuk umum. Bahaya dapat berhubungan dengan privasi individu, posisi bisnis strategis Energizer atau pelanggan, atau kewajiban hukum atau peraturan. Sesuai dengan peran dan tanggung jawab Anda, Anda mungkin memiliki akses ke data rahasia Energizer.

Contoh data rahasia meliputi rencana strategis, rencana pemasaran, data keuangan, daftar pelanggan, kontrak, rencana bisnis, paten yang tidak dipublikasikan, rahasia dagang, dokumentasi M&A, informasi yang tunduk pada perjanjian non-pengungkapan, atau informasi teknis atau bisnis lainnya.

Kebijakan ini mensyaratkan perlindungan data rahasia dalam penyimpanan, penyebaran, dan pembagian baik di dalam maupun di luar perusahaan menggunakan pengamanan administratif,

fisik, dan teknis yang sesuai dengan risiko yang ditimbulkan oleh kemungkinan akses tidak sah ke data.

4.1 Tanggung jawab Anda untuk melindungi data perusahaan

Kecuali jika ditandai sebaliknya atau jelas dimaksudkan sebagai informasi publik, perlakukan semua informasi/data seolah-olah itu data rahasia Energizer, terlepas dari sumber atau bentuknya, termasuk informasi elektronik, kertas, verbal, atau lainnya.

Energizer menetapkan panduan berikut untuk mengakses, menyimpan, dan/atau mentransmisikan (yaitu, memproses) file yang berisi data rahasia Energizer:

- Secara mencolok menandai semua dokumen, file, atau email yang berisi data rahasia Energizer dengan yang berikut:

“Kepemilikan dan rahasia Energizer”

- File yang berisi jenis data ini hanya boleh disimpan di lokasi yang aman seperti OneDrive, tetapi dapat disimpan sementara di sumber daya perusahaan yang aman seperti komputer laptop atau desktop, yang akhirnya disimpan di OneDrive.
- Lindungi data rahasia dengan enkripsi dan/atau kata sandi yang sesuai dan hanya kirim menggunakan metode aman, seperti enkripsi baris subjek, Citrix ShareFile, atau portal transmisi aman.
- Ingatlah untuk mengunci komputer Anda jika Anda perlu menjauh darinya.
- Jangan meninggalkan laptop Anda di depan mata, atau tanpa jaminan, di mobil Anda atau kamar hotel dan jangan berjalan menjauh dari itu di lokasi umum seperti bandara.
- Data rahasia harus dihapus dari komputer Anda segera setelah Anda tidak lagi memiliki kebutuhan untuk mengaksesnya, kecuali tunduk pada penangguhan litigasi atau lainnya untuk mematuhi jadwal penyimpanan catatan Energizer.
- Hanya mendiskusikan data rahasia di tempat-tempat non-publik atau dengan mengambil langkah-langkah yang wajar untuk menghindari didengar.
- Hanya memindai, mendistribusikan, menyalin, dan mendistribusikan data rahasia sejauh yang diperlukan, dan memastikan pihak penerima tunduk pada perjanjian non-pengungkapan atau di bawah kewajiban kerahasiaan yang serupa.

Kembalikan semua data rahasia yang Anda miliki di akhir pekerjaan Anda dan ingat bahwa kewajiban Anda untuk melindungi data rahasia bertahan melewati pemutusan hubungan kerja. **Jika Anda mengetahui bahwa data rahasia dibagikan dengan pihak yang tidak berwenang (sengaja atau tidak sengaja), atau laptop atau perangkat seluler Anda hilang, dicuri, atau dikompromikan dan berisi data rahasia, silakan hubungi Kepala Etika & Kepatuhan dan staf TI segera untuk melaporkan insiden tersebut.**

Punya pertanyaan atau kekhawatiran?



Kebijakan Perlindungan data Global

Tanggal efektif: 2018 Februari

Revisi terakhir: April 2025

Ada banyak cara untuk mengajukan pertanyaan atau menimbulkan kekhawatiran mengenai kebijakan ini. Pilih opsi yang paling nyaman Anda gunakan. Apapun pilihan yang Anda pilih, kerahasiaan Anda akan dihormati, dan pembalasan tidak akan ditoleransi:

- Manajer Anda atau kepemimpinan tingkat berikutnya
- Sumber daya manusia
- Etika & Kepatuhan energizercompliance@energizer.com
- Legal
- Saluran bantuan Energizer: www.EnergizerHelpLine.com
 - Hubungi 1-877-521-5625 (AS)
 - Nomor telepon tambahan di www.EnergizerHelpLine.com
 - Teks "laporan" ke 314-668-1383 (hanya Amerika Utara)
 - anda dapat tetap anonim jika anda memilih
 - tersedia 24 jam dan dioperasikan oleh penyedia pihak ke-3rd

Section 5: Kebijakan dan standar terkait

Nama kebijakan
Kode Etik Kebijakan penggunaan teknologi informasi yang dapat diterima Kebijakan Records and Information Management (RIM)

Section 6: Riwayat Revisi

Pemilik kebijakan akan meninjau dan memperbarui kebijakan ini seperlunya setidaknya sekali setiap tahun fiskal.

Nomor revisi	Tanggal efektif	Pemilik	Deskripsi perubahan
4	Tanggal 2024 April	Seth Smoker	Pemilik Kebijakan yang diperbarui; mengubah "Kepala Etika & Kepatuhan" menjadi "Penasihat umum Associate, Etika & Kepatuhan Global" dan mengubah informasi kontak menjadi Karen Benson
3	Maret 2021	Ronnie Kann	Informasi kontak terbaru untuk saluran bantuan Energizer
2	Tanggal 2020 November	Ronnie Kann	Pemilik kebijakan yang diperbarui; mengubah "petugas kepatuhan utama" menjadi "kepala etika & kepatuhan"; menambahkan cara mengajukan pertanyaan atau menimbulkan kekhawatiran; menambahkan kebijakan RIM dan Kode Etik ke kebijakan dan standar terkait
1	Tanggal 2018 Januari	Kathy Rehmer	Kebijakan baru



Kebijakan Perlindungan data Global

Tanggal efektif: 2018 Februari

Revisi terakhir: April 2025

Section 7: Persetujuan yang diperlukan

Tanda tangan pada file _____

Tanda tangan pada file _____

Section 1: Tujuan daripada kebijakan ini

Dasar Perlindungan Data Global ini ("Dasar") menggalakkan keseimbangan yang berkesan antara amalan keselamatan maklumat dan keperluan perniagaan, sambil mengekalkan pematuhan dengan undang-undang yang berkaitan. Dasar ini membantu Energizer memenuhi kewajipan undang-undang kami sambil mengekalkan keupayaan untuk perniagaan menjadi tangkas dan memenuhi jangkaan pelanggan. Seperti yang dinyatakan di bawah dengan lebih terperinci, Energizer memerlukan tahap kawalan keselamatan yang berbeza bergantung kepada klasifikasi maklumat yang akan dilindungi, yang berdasarkan risiko, praktikal dan pertimbangan lain.

Pelanggan, rakan sekerja, dan lain-lain bergantung kepada kami untuk melindungi maklumat mereka. Pelanggaran keselamatan data boleh merosakkan kredibiliti kami dengan teruk, menyebabkan kehilangan perniagaan dan bahaya lain kepada individu yang terjejas. Keselamatan data yang kukuh memerlukan ketekunan semua rakan sekerja, kontraktor dan mana-mana pihak lain yang mengakses atau menggunakan aset data kami. Perlindungan data adalah sebahagian daripada kerja semua orang.

Asas-asas bimbingan

Semua rakan sekerja perlu mengambil kira prinsip-prinsip berikut untuk perlindungan data:

- i. Energizer melindungi kerahsiaan, integriti dan akses kepada aset datanya.
- ii. Energizer akan mematuhi undang-undang privasi data dan perlindungan data yang berkenaan.
- iii. Energizer mengimbangi keperluan untuk kecekapan perniagaan dengan keperluan untuk melindungi maklumat peribadi, proprietari dan maklumat sulit lain daripada risiko yang tidak perlu.
- iv. Energizer hanya memberikan akses kepada maklumat peribadi, proprietari dan lain-lain maklumat sulit kepada mereka yang perlu tahu dan yang diwajibkan untuk mengekalkan keselamatan maklumat.
- v. Rakan sekerja Energizer merupakan barisan pertahanan pertama dan terbaik terhadap insiden keselamatan data, dan ia merupakan tanggungjawab setiap rakan sekerja untuk menegakkan amalan Dasar ini.
- vi. Rangkaian, sistem dan aset Energizer terutamanya untuk tujuan perniagaan. Kecuali jika undang-undang yang berkenaan menyediakan sebaliknya, anda tidak boleh mengharapkan privasi apabila menggunakan rangkaian atau sistem Energizer, termasuk, tetapi tidak terhad kepada, menghantar dan menyimpan fail, data, dan mesej.

Section 2: Ahli politik dan pernyataan tanggungjawab

Dasar ini dimiliki oleh Penasihat Am Bersekutu, Etika Global & Pematuhan. Ia merupakan tanggungjawab individu ini, bersama-sama dengan undang-undang, untuk melaksanakan, mengkaji semula setiap tahun, dan menyemak semula dasar ini seperti yang diperlukan.

Nama	Tajuk	Telefon	E-mel
Karen Benson	Penasihat Am Bersekutu, Etika & Pematuhan Global	954.593.6876	karen.benson@energizer.com

Section 3: Melindungi maklumat peribadi**3.1 Pengumpulan & Pemprosesan Data rakan Sekerja**

Untuk menjalankan perniagaannya dengan berkesan, Energizer perlu mengumpul dan menggunakan maklumat peribadi tertentu mengenai rakan sekerja kami. Undang-undang dan peraturan privasi data global memerlukan pengumpulan, penyimpanan, pemprosesan, perkongsian, pemindahan dan penggunaan data peribadi yang sesuai, termasuk data peribadi rakan sekerja ("Data Peribadi rakan Sekerja"). Ia merupakan tanggungjawab asas rakan sekerja, seperti yang digariskan dalam Tatakelakuan, untuk menggunakan data hanya untuk tujuan yang dimaksudkan dan untuk melindungi data ini dengan sewajarnya.

Data tertentu, termasuk data peribadi sensitif dan data peribadi, dikumpulkan daripada rakan sekerja - dan dalam beberapa keadaan calon untuk pekerjaan - sama ada oleh pihak ketiga yang diberi kuasa syarikat atau syarikat untuk mentadbir semua aspek pekerjaan, termasuk tetapi tidak terhad kepada: Gaji, pampasan, perjalanan, pembayaran balik perbelanjaan, pemberian dalam talian, pentadbiran faedah, prosedur disiplin dan keluhan, masa & kehadiran, pengurusan kursus latihan, dan pengurusan kerjaya.

Apabila perlu untuk tujuan perniagaan, dan dibenarkan oleh undang-undang, Energizer juga boleh mengakses dan menyimpan e-mel dan dokumen, termasuk resume (CV), yang mungkin mengandungi data peribadi atau sensitif. Energizer juga boleh mengumpul data rakan sekerja apabila ia memantau komunikasi dan sistem untuk melindungi perniagaan daripada virus dan perisian hasad atau untuk memastikan pematuhan dengan dasar, undang-undang dan peraturan.

3.2 Jenis Data rakan Sekerja dikumpulkan**3.2(a) Maklumat Peribadi**

Di Kesatuan Eropah (EU) dan banyak negara lain, "data peribadi" ditakrifkan secara meluas sebagai apa-apa maklumat yang berkaitan dengan orang yang dikenal pasti atau boleh dikenal pasti (iaitu, orang yang boleh dikenal pasti secara langsung atau tidak langsung dengan merujuk kepada nama, nombor ID, dan lain-lain). Ringkasnya, data peribadi boleh termasuk nama seseorang, alamat e-mel, alamat fizikal, atau sejenisnya.

3.2(b) Maklumat Peribadi sensitif

Undang-undang privasi data berbeza-beza mengikut negara dan beberapa elemen data dianggap sensitif dalam bidang kuasa tertentu dan memerlukan perlindungan tambahan kerana penggunaan data yang tidak sesuai boleh menyebabkan kecurian identiti. Sebagai contoh, Data Peribadi sensitif mungkin termasuk:

- Maklumat akaun bank atau kad kredit (seperti nombor akaun dan nombor penghasilan)
- ID Kebangsaan, seperti nombor Keselamatan Sosial
- Pasport #
- Gaji dan maklumat pampasan yang berkaitan
- Biometrik, maklumat kesihatan dan perubatan
- Ras atau etnik asal
- Kepercayaan politik mahupun agama
- Ahli-ahli persatuan

3.3 Undang-undang Perlindungan Data

Banyak negara telah mengisytiharkan undang-undang privasi data yang menyatakan keperluan untuk "memproses" data peribadi. "Pemprosesan" boleh termasuk tindakan seperti mengumpul, menggunakan, menyimpan, mengubah, mendedahkan, atau menghantar maklumat peribadi, antara lain. Sebagai contoh, pemprosesan data peribadi warga EU (termasuk rakan sekerja & pemohon) dikawal selia supaya mana-mana pengumpulan data, pemprosesan, atau pemindahan di luar EU (atau negara-negara lain yang diluluskan) mesti mematuhi undang-undang, seperti Peraturan Perlindungan Data Am EU (GDPR).

Sebarang pemindahan data peribadi EU di luar Kesatuan Eropah - termasuk mengakses data peribadi EU dari luar EU - memerlukan perlindungan yang sesuai sebelum pemindahan data. Di samping itu, berkongsi data peribadi EU dengan pihak ketiga (walaupun mereka yang mempunyai kontrak dengan) di luar EU memerlukan keselamatan yang sesuai dan harus diselaraskan dengan undang-undang dan Ketua Etika & Pematuhan.

3.4 - Tanggungjawab anda untuk melindungi Data rakan Sekerja

Rakan sekerja dan kontraktor diwajibkan mematuhi semua aspek Dasar ini yang terpakai kepada mereka. Jika anda mempunyai akses kepada Data Peribadi dan/atau Data Peribadi sensitif, atau data individu lain berdasarkan peranan anda dalam Syarikat, adalah menjadi tanggungjawab anda untuk melaksanakan kawalan yang diluluskan oleh Energizer untuk melindungi dan melindungi data tersebut dan mengehadkan akses kepada data tersebut kepada hanya mereka yang mempunyai keperluan untuk mengetahui dan hanya untuk tujuan perniagaan yang perlu dan sah.

Energizer menetapkan garis panduan berikut untuk rakan sekerja yang mengakses, menyimpan dan/atau menghantar (iaitu, memproses) fail dengan Data Peribadi atau Data Peribadi sensitif:

- i. Tandakan semua dokumen, fail atau e-mel yang mengandungi Data Peribadi sensitif dengan tanda berikut:

"Peribadi dan Sulit"

Dasar Perlindungan Data Global

Tarikh berkuatkuasa: Februari 2018

Tarikh Kemaskini: April 2025

-
- ii. Fail yang mengandungi jenis data ini hanya boleh disimpan di lokasi yang selamat seperti OneDrive, tetapi boleh disimpan **sementara** pada sumber syarikat yang dijamin seperti komputer riba atau komputer desktop, akhirnya disimpan dalam OneDrive.
 - iii. Lindungi fail Data Peribadi sensitif dengan penyulitan dan/atau kata laluan. Fail Data Peribadi sensitif hanya boleh dihantar menggunakan kaedah selamat/disulitkan, seperti penyulitan baris subjek, Citrix ShareFile atau portal penghantaran selamat dengan vendor.
 - iv. Sebelum berkongsi Data Peribadi EU dan Data Peribadi sensitif dengan pihak ketiga, pastikan bahawa ia sesuai dan perlu dan hubungi sumber Privasi di bawah untuk memastikan perlindungan yang sesuai disediakan.
 - v. Jangan lupa untuk mengunci komputer anda jika anda perlu keluar daripadanya.
 - vi. Jangan tinggalkan komputer riba anda dalam keadaan biasa, atau tidak selamat, di dalam kereta anda atau bilik hotel dan jangan berjalan kaki daripadanya di lokasi awam seperti lapangan terbang.
 - vii. Sila ambil perhatian bahawa data seperti nama, alamat e-mel, dan maklumat lain yang berkaitan dengan orang yang dikenal pasti atau boleh dikenal pasti boleh dianggap sebagai "Data Peribadi" di bawah undang-undang privasi banyak negara dan mungkin memerlukan perlindungan tambahan.
 - viii. Data harus dipadamkan dari komputer anda sebaik sahaja anda tidak lagi mempunyai keperluan untuk mengaksesnya, melainkan tertakluk kepada penahanan litigasi atau jadual pengekalan rekod lain.

Akhir sekali, beritahu Ketua Etika & Pematuhan jika anda tidak pasti jika maklumat atau fail tertentu boleh dikongsi dengan pihak lain, jika anda menyedari maklumat sensitif yang dikongsi secara tidak sengaja, atau tidak dibenarkan, atau jika komputer riba atau peranti mudah alih anda (telefon atau tablet) telah hilang, dicuri atau dikompromi. Komputer riba atau peranti mudah alih yang dicuri juga perlu dilaporkan kepada Concierge IT.

Section 4: Melindungi Data Peribadi atau Data Peribadi Syarikat

Data Rahsia Energizer

Maklumat sulit adalah maklumat yang boleh menyebabkan kemudaratan kepada Accenture, pelanggan, rakan sekerja, atau entiti atau individu lain jika didedahkan secara tidak wajar, atau maklumat yang tidak tersedia secara umum. Kemudaratan mungkin berkaitan dengan privasi individu, kedudukan perniagaan strategik Energizer atau pelanggan, atau liabiliti undang-undang atau peraturan. Selaras dengan peranan dan tanggungjawab anda, anda mungkin mempunyai akses kepada Data Rahsia Energizer.

Contoh Data Sulit termasuk pelan strategik, pelan pemasaran, data kewangan, senarai pelanggan, kontrak, pelan perniagaan, paten yang tidak diterbitkan, rahsia perdagangan, dokumentasi M & A, maklumat tertakluk kepada perjanjian bukan pendedahan, atau maklumat teknikal atau perniagaan lain.

Dasar ini memerlukan perlindungan data sulit dalam penyimpanan, penyebaran dan perkongsian di dalam dan di luar syarikat menggunakan perlindungan pentadbiran, fizikal, dan teknikal yang sesuai mengikut risiko yang ditimbulkan oleh akses yang tidak dibenarkan kepada data.

4.1 Tanggungjawab anda untuk melindungi data syarikat

Melainkan ia ditandakan sebaliknya atau dengan jelas bertujuan untuk menjadi maklumat Awam, anggap semua maklumat/data seolah-olah ia Data Sulit Google, tanpa mengira sumber atau bentuknya, termasuk maklumat elektronik, kertas, lisan atau lain-lain.

Energizer menetapkan garis panduan berikut untuk mengakses, menyimpan dan/atau menghantar (iaitu, memproses) fail yang mengandungi Data Sulit Energizer:

- Tandakan semua dokumen, fail atau e-mel yang mengandungi Data Sulit Energizer dengan jelas seperti berikut:

"Energizer proprietari dan Sulit"

- Fail yang mengandungi jenis data ini hanya boleh disimpan di lokasi yang selamat seperti OneDrive, tetapi boleh disimpan sementara pada sumber syarikat yang dijamin seperti komputer riba atau komputer desktop, akhirnya disimpan dalam OneDrive.
- Lindungi Data Sulit dengan penyulitan dan/atau kata laluan yang sesuai dan hanya hantar menggunakan kaedah yang selamat, seperti penyulitan baris subjek, Citrix ShareFile atau portal penghantaran yang selamat.
- Jangan lupa untuk mengunci komputer anda jika anda perlu keluar daripadanya.
- Jangan tinggalkan komputer riba anda dalam keadaan biasa, atau tidak selamat, di dalam kereta anda atau bilik hotel dan jangan berjalan kaki daripadanya di lokasi awam seperti lapangan terbang.
- Data Sulit harus dipadamkan dari komputer anda sebaik sahaja anda tidak lagi mempunyai keperluan untuk mengaksesnya, melainkan tertakluk kepada penahanan litigasi atau lain-lain untuk mematuhi jadual pengekalan rekod Energizer.
- Hanya membincangkan Data sulit di tempat bukan awam atau dengan mengambil langkah yang munasabah untuk mengelakkan didengar.
- Hanya mengimbas, mengedarkan, menyalin dan mengedarkan Data Sulit setakat yang perlu, dan memastikan pihak penerima tertakluk kepada perjanjian bukan pendedahan atau di bawah kewajipan kerahsiaan yang sama.

Kembalikan semua Data Sulit dalam pemilikan anda pada akhir pekerjaan anda dan ingat bahawa kewajipan anda untuk melindungi data sulit bertahan selepas penamatan pekerjaan. **Jika anda menyedari bahawa Data Sulit telah dikongsi dengan pihak yang tidak dibenarkan (secara sengaja atau tidak sengaja), atau komputer riba atau peranti mudah alih anda telah hilang, dicuri atau dikompromi dan ia mengandungi**

Dasar Perlindungan Data Global

Tarikh berkuatkuasa: Februari 2018

Tarikh Kemaskini: April 2025

Data Sulit, sila hubungi Ketua Etika & Pematuhan dan PERKHIDMATAN IT dengan segera untuk melaporkan kejadian tersebut.

Mempunyai soalan atau kebimbangan?

Terdapat banyak cara untuk bertanya soalan atau menimbulkan kebimbangan mengenai dasar ini. Pilih pilihan yang anda paling selesa digunakan. Mana-mana pilihan yang anda pilih, kerahsiaan anda akan dihormati, dan tindakan balas tidak akan diterima:

- Pengurus anda atau kepimpinan peringkat seterusnya
- Sumber manusia
- Etika dan Perkhidmatan energizercompliance@energizer.com
- Undang-undang
- Kuasa enjin: www.EnergizerHelpLine.com
 - Hubungi 1-877-521-5625 (A.S.)
 - Nombor telefon tambahan di www.EnergizerHelpLine.com
 - Teks "Laporan" kepada 314-668-1383 (Amerika Utara sahaja)
 - anda boleh kekal tanpa nama jika anda memilih
 - tersedia 24 jam dan dikendalikan oleh pembekal pihak ke-3

Section 5: Undang-undang dan peraturan yang berkaitan

Nama dasar
Tatakelakuan Teknologi maklumat Dasar penggunaan boleh diterima Pengurusan rekod dan maklumat (RIM)

Section 6: Sejarah Semakan

Pemilik dasar akan menyemak semula dan mengemas kini dasar ini jika perlu sekurang-kurangnya sekali setiap tahun fiskal.

Nombor Semakan	Tarikh efektif	Pemilik	Menerangkan perubahan
4	2024 April	Seth Smoker	Pemilik Dasar yang dikemas kini; menukar "ketua etika & pematuhan" kepada "Penasihat Am Bersekutu, Etika & Pematuhan Global" dan menukar maklumat hubungan kepada Karen Benson
3	2021 Mac	Ronnie Kann	Maklumat hubungan terkini untuk talian bantuan Energizer
2	2020 November	Ronnie Kann	Pemilik dasar yang dikemas kini; menukar "ketua pegawai pematuhan" kepada "ketua etika & pematuhan"; menambah cara untuk bertanya soalan atau menimbulkan



Dasar Perlindungan Data Global

Tarikh berkuatkuasa: Februari 2018

Tarikh Kemaskini: April 2025

			keimbangan; menambah dasar RIM dan Tatakelakuan kepada dasar dan standard yang berkaitan
1	Januari 2018	Kathy Rehmer	Politik baru

Section 7: Kelulusan yang diperlukan

Tandatangan pada fail _____

Tandatangan pada fail _____



全球数据保护政策

生效日期：2018年2月

最后修订日期:2025年4月

Section 1: 本政策的目 的

本全球数据保护政策(以下简称"政策")促进信息安全实践与业务需求之间的有效平衡,同时保持对相关法律法规的遵守。该政策有助于劲量履行我们的法律义务,同时保持业务敏捷性和满足客户期望的能力。如下文更详细地阐述的那样,劲量根据要保护的信息的分类(基于风险,实用性和其他考虑因素)要求不同级别的安全控制。

我们的客户,同事和其他人依赖我们来保护他们的信息。数据安全漏洞可能会严重损害我们的信誉,导致业务流失和对受影响的个人造成其他伤害。强大的数据安全要求访问或使用我们数据资产的所有同事,承包商和任何其他人都尽职尽责。数据保护是每个人工作的一部分。

指导原则

所有同事都应牢记以下数据保护原则:

- i. 劲量保护其数据资产的机密性,完整性和访问权限。
- ii. 劲量将遵守适用的数据隐私和数据保护法。
- iii. 劲量在业务效率需求与保护个人,专有和其他机密信息免受不必要风险的需求之间取得平衡。
- iv. 劲量仅授予那些需要知道并有义务维护信息安全的人访问个人,专有和其他机密信息的权限。
- v. 劲量员工是应对数据安全事件的第一道防线,也是最佳防线,每位员工都有责任维护本政策的实践。
- vi. 劲量的网络,系统和其他资产主要用于业务目的。除非适用法律另有规定,否则您在使用劲量网络或系统时,包括但不限于传输和存储文件,数据和消息时,不应期望隐私。

Section 2: 政策所有者和责任声明

本政策归全球道德与合规部副总法律顾问所有。此人有责任与法务部一起实施,每年审查并根据需要修订此政策。



全球数据保护政策

生效日期：2018年2月

最后修订日期:2025年4月

名称	标题	电话	电子邮件
Karen Benson	全球道德与合规部副总法律顾问	954.593.6876	karen.benson@energizer.com

Section 3: 保护个人数据

3.1 员工数据的收集和处理

为了有效开展业务，劲量需要收集和使用有关我们同事的某些个人信息。全球数据隐私法律和法规要求适当收集，存储，处理，共享，传输和使用个人数据，包括同事的个人数据("同事个人数据")。如行为准则中所述，同事有基本责任仅将数据用于预期目的，并适当保护这些数据。

某些数据(包括敏感的个人数据和敏感数据)由公司或公司授权的第三方从同事(有时是应聘者)收集，以管理雇佣的各个方面，包括但不限于：工资，薪酬，差旅，费用报销，在线赠送，福利管理，纪律和申诉程序，时间和出勤，培训课程管理和职业管理。

出于商业目的需要且法律允许时，劲量还可能访问和存储可能包含个人或敏感数据的电子邮件和文档，包括简历(CV)。劲量还可能在监控通信和系统时收集同事数据，以保护企业免受病毒和恶意软件的侵害，或确保遵守政策，法律和法规。

3.2 收集的同事数据类型

3.2(a) –个人数据

在欧盟(EU)和许多其他国家，"个人数据"被广泛定义为与已识别或可识别的个人(即可通过参考姓名，身份证号码等直接或间接识别的个人)有关的任何信息。简而言之，个人数据可以包括个人的姓名，电子邮件地址，实际地址等。

3.2(b) –敏感个人数据

数据隐私法因国家/地区而异，某些数据元素在某些司法管辖区被视为敏感，需要额外保护，因为不当使用这些数据可能导致身份盗窃。例如，敏感个人数据可能包括：



全球数据保护政策

生效日期：2018年2月

最后修订日期:2025年4月

- 银行账户或信用卡信息(如账号和转账号码)
- 身份证件，如社会保险号
- 护照号码
- 薪资和相关薪酬信息
- 生物鉴别，健康和医疗信息
- 种族或民族血统
- 政治或宗教信仰
- 工会会员资格

3.3 数据保护法

许多国家颁布了数据隐私法，规定了"处理"个人数据的要求。"处理"可包括收集，使用，存储，更改，披露，或传输个人数据等。例如，欧盟公民(包括同事和申请人)的个人数据处理受到监管，任何数据收集，处理或在欧盟(或其他批准国家/地区)以外传输必须遵守法律，例如欧盟一般数据保护条例(GDPR)。

在欧盟以外传输欧盟个人数据(包括从欧盟以外访问欧盟个人数据)需要在数据传输之前采取适当的保护措施。此外，与欧盟以外的第三方(即使是我们与之签订合同的第三方)共享欧盟个人数据需要适当的安全性，并且应与法务部和道德与合规部主管协调。

3.4 –您有责任保护同事数据

同事和承包商有义务遵守适用于他们的本政策的所有方面。如果您可以访问个人数据和/或敏感个人数据，或基于您在公司的角色的其他个人数据，您有责任实施适当批准的控制措施，以保护和保护该数据，并将数据访问限制为仅限于需要知晓且仅用于必要和合法业务目的的人员。

适当为访问，保存和/或传输(即处理)包含个人数据或敏感个人数据的文件的同事制定了以下准则：

- i. 用以下标记明显标记包含敏感个人数据的所有文档，文件或电子邮件：

"个人和机密"



全球数据保护政策

生效日期：2018 年 2 月

最后修订日期:2025 年 4 月

- ii. 包含此类数据的文件只应保存在安全位置(如 OneDrive), 但可能会临时存储在安全的公司资源(如便携式计算机或台式计算机)上, 最终存储在 OneDrive 中。
- iii. 使用加密和/或密码保护敏感个人数据文件。敏感个人数据文件只能使用安全/加密的方法传输,例如主题行加密, Citrix ShareFile 或供应商的安全传输门户。
- iv. 在与第三方共享欧盟个人数据和敏感个人数据之前, 请确保这是适当和必要的, 并联系下面的隐私资源以确保实施适当的保护措施。
- v. 如果您需要远离计算机, 请记住锁定计算机。
- vi. 切勿将笔记本电脑放在眼前或不安全的地方, 将其放在汽车或酒店房间, 也不要再在机场等公共场所离开。
- vii. 请注意, 根据许多国家的隐私法, 即使是姓名, 电子邮件地址和与已识别或可识别人员相关的其他信息, 也可能被视为"个人数据", 并且可能需要额外的保护。
- viii. 一旦您不再需要访问数据, 应立即从您的计算机中删除数据, 除非受到诉讼保留或其他记录保留计划的约束。

最后, 如果您不确定某些信息或文件是否可以与另一方共享, 如果您发现错误共享或未经授权共享的敏感信息, 或者您的笔记本电脑或移动设备(手机或平板电脑)丢失, 被盗或泄露, 请通知道德与合规部主管。被盗的笔记本电脑或移动设备也应报告给 IT 礼宾部。

Section 4: 保护公司机密或专有数据

劲量机密数据

机密信息是指因不当披露而可能对劲量, 其客户, 同事或其他实体或个人造成损害的信息, 或以其他方式未公开的信息。损害可能涉及个人的隐私, 劲量的战略业务地位或客户的战略业务地位, 或法律或监管责任。根据您的角色和职责, 您可以访问劲量机密数据。

机密数据的示例包括战略计划, 营销计划, 财务数据, 客户名单, 合同, 商业计划, 未公布的专利, 商业秘密, 并购文档, 保密协议约束的信息或其他技术或商业信息。

本政策要求在公司内部和外部存储, 传播和共享机密数据时, 根据可能的未经授权访问数据带来的风险, 采取适当的管理, 物理和技术保护措施。



全球数据保护政策

生效日期：2018 年 2 月

最后修订日期:2025 年 4 月

4.1 您保护公司数据的责任

除非另有标记或明确意图为公共信息，否则应将所有信息/数据视为劲量机密数据，无论其来源或形式如何，包括电子，纸质，口头或其他信息。

劲量为访问，保存和/或传输(即处理)包含劲量机密数据的文件制定了以下准则：

- 在所有包含劲量机密数据的文档，文件或电子邮件中显著标记以下内容：



全球数据保护政策

生效日期：2018 年 2 月

最后修订日期:2025 年 4 月

"Energizer 专有和机密"

- 包含此类数据的文件只应保存在安全位置(如 OneDrive)，但可能会临时存储在安全的公司资源(如便携式计算机或台式计算机)上，最终存储在 OneDrive 中。
- 使用适当的加密和/或密码保护机密数据,并且只能使用安全方法(如主题行加密，Citrix ShareFile 或安全传输门户)进行传输。
- 如果您需要远离计算机，请记住锁定计算机。
- 切勿将笔记本电脑放在眼前或不安全的地方，将其放在汽车或酒店房间，也不要再在机场等公共场所离开。
- 一旦您不再需要访问机密数据，应立即从您的计算机中删除机密数据，除非因遵守劲量记录保留时间表而受到诉讼保留或采取其他措施。
- 仅在非公开场所讨论机密数据，或采取合理措施避免被听到。
- 仅在必要范围内扫描，分发，复制和分发机密数据，并确保接收方遵守保密协议或类似的保密义务。

在雇佣关系结束时返还您拥有的所有机密数据，并记住，您保护机密数据的义务在雇佣关系终止后仍然有效。如果您发现机密数据与未授权方共享(有意或无意)，或者您的笔记本电脑或移动设备丢失，被盗或泄露且包含机密数据，请立即联系道德与合规部主管和 IT 礼宾部，报告此事件。

有疑问或顾虑吗？

有许多方法可以就这项政策提问或提出疑虑。选择您最喜欢使用的选项。无论您选择哪一种选择，您的保密性都将得到尊重，并且绝不容忍报复：

- 您的经理或上一级领导
- 人力资源
- 道德与合规 energizercompliance@energizer.com
- 法律
- Energizer 帮助热线：www.EnergizerHelpLine.com
 - 致电 1-877-521-5625 (美国)
 - www.EnergizerHelpLine.com 上的其他电话号码



全球数据保护政策

生效日期：2018 年 2 月

最后修订日期:2025 年 4 月

- 文本"报告"至 314-668-1383 (仅限北美)
- 如果您选择，您可以保持匿名
- 24 小时提供服务，由第三方提供商运营

Section 5: 相关政策和标准

策略名称
行为准则
信息技术可接受使用政策
记录和信息管理(RIM)策略

Section 6: 修订历史记录

保单所有者将在必要时至少每财年审查和更新此保单一次。

修订版本号	生效日期	所有者	更改说明
4	2024 年 4 月	塞斯吸烟者	更新了政策负责人；将"道德与合规部主管"更改为"全球道德与合规部协理总顾问"，并将联系人信息更改为 Karen Benson
3	2021 年 3 月	Ronnie Kann	更新了 Energizer 帮助热线的联系信息
2	2020 年 11 月	Ronnie Kann	更新策略所有者；将"首席合规官"更改为"道德与合规主管"；添加了如何提问或提出顾虑的内容；将 RIM 政策和行为准则添加到相关策略和标准中
1	2018 年 1 月	Kathy Rehmer	新政策

Section 7: 所需的批准

文件中的签名_____

文件中的签名_____

Deel 1: Doel van dit beleid

Dit Algemene Gegevensbeschermingsbeleid (het "Beleid") is gericht op het realiseren een effectief evenwicht tussen informatiebeveiligingspraktijken en zakelijke behoeften, in overeenstemming met de toepasselijke wetgeving. Het Beleid helpt Energizer te voldoen aan onze wettelijke verplichtingen, terwijl de onderneming de mogelijkheid behoudt om flexibel te zijn en te voldoen aan de verwachtingen van de klant. Zoals hieronder in meer detail uiteengezet, vereist Energizer verschillende niveaus van beveiligingscontroles, afhankelijk van de classificatie van de te beschermen informatie, die gebaseerd is op risico, uitvoerbaarheid en andere overwegingen.

Onze klanten, collega's en anderen vertrouwen erop dat wij hun informatie beschermen. Een inbreuk op de gegevensbeveiliging kan onze geloofwaardigheid ernstig schaden, verlies van zaken veroorzaken en andere schade toebrengen aan getroffen personen. Een sterke gegevensbeveiliging vereist zorgvuldigheid van alle collega's, aannemers en anderen die toegang hebben tot onze gegevens of deze gebruiken. Gegevensbescherming maakt deel uit van ieders werk.

Richtlijnen

Alle collega's zijn gehouden de volgende principes voor gegevensbescherming te respecteren:

- i. Energizer beschermt de vertrouwelijkheid, integriteit en toegang tot haar datamiddelen.
- ii. Energizer zal voldoen aan de toepasselijke wetgeving inzake privacy en gegevensbescherming.
- iii. Energizer balances the needs for business efficiency with the need to protect personal, proprietary and other confidential information from unnecessary risk.
- iv. Energizer only grants access to personal, proprietary and other confidential information to those with a need to know and who are obligated to maintain the security of the information.
- v. Energizer colleagues are the first and best line of defense against data security incidents, and it is every colleague's responsibility to uphold the practices of this Policy.
- vi. Energizer's network, systems and other assets are primarily for business purposes. Except where applicable law provides otherwise, you should have no expectation of privacy when using Energizer's network or systems, including, but not limited to, transmitting and storing files, data, and messages.

Deel 2: Policy Owner and Statement of Responsibility

Dit Beleid werd uitgevaardigd door het hoofd van Ethics & Compliance. Het is de verantwoordelijkheid van deze persoon, samen met Legal, om dit Beleid te implementeren, jaarlijks te herzien en waar nodig te herzien.

Name	Title	Phone	Email
Karen Benson	General Counsel van medewerkers, Global Ethics & Compliance	954.593.6876	karen.benson@energizer.com

Deel 3: Persoonsgegevens beschermen

3.1 Verzameling en verwerking van Persoonsgegevens van Collega's

Voor een efficiënte bedrijfsvoering, moet Energizer bepaalde persoonlijke informatie over onze collega's verzamelen en gebruiken. Internationale wetgeving omtrent gegevensbescherming vereisen het op gepaste wijze verzamelen, opslaan, verwerken, delen, overdragen en gebruiken van persoonsgegevens, inclusief de persoonsgegevens van collega's ("Persoonsgegevens van Collega's"). Het is de fundamentele verantwoordelijkheid van collega's, zoals uiteengezet in de Gedragscode, om de gegevens alleen te gebruiken voor het doel waarvoor ze bedoeld zijn en om deze gegevens op de juiste manier te beschermen.

Bepaalde gegevens, waaronder persoonsgegevens en gevoelige persoonsgegevens, worden verzameld van collega's - en in sommige gevallen van kandidaten - door de onderneming of door bevoegde derden van de ondernemingen om alle aspecten van het dienstverband te beheren, waaronder, maar niet beperkt tot:

salarisadministratie, vergoedingen, reizen, onkostenvergoedingen, online diensten, voordelenadministratie, disciplinaire en klachtenprocedures, tijdregistratie, beheer van trainingscursussen en loopbaanbeheer.

Indien nodig voor zakelijke doeleinden, en toegestaan door de wetgeving, kan Energizer ook e-mails en documenten openen en opslaan, inclusief CV's, die persoons- of gevoelige gegevens kunnen bevatten. Energizer kan ook Persoonsgegevens van Collega's verzamelen wanneer het de communicatie en systemen controleert om de onderneming te beschermen tegen virussen en malware of om naleving van beleid, wetgeving en regelgeving te verzekeren.

3.2 Soorten verzamelde Persoonsgegevens van Collega's

3.2(a) – Persoonsgegevens

In de Europese Unie (EU) en veel andere landen worden "persoonsgegevens" ruim gedefinieerd als alle informatie over een geïdentificeerde of identificeerbare persoon (d.w.z. een persoon die direct of indirect kan worden geïdentificeerd aan de hand van een naam, ID-nummer, enz.). Eenvoudig gezegd kunnen persoonsgegevens iemands naam, e-mailadres, fysiek adres en dergelijke omvatten.

3.2(b) – Gevoelige Persoonsgegevens

Gegevensbeschermingswetgeving verschilt per land en sommige gegevenselementen worden in bepaalde rechtsgebieden als gevoelig beschouwd en vereisen extra bescherming omdat ongepast gebruik van deze gegevens tot identiteitsdiefstal kan leiden. Gevoelige persoonsgegevens kunnen bijvoorbeeld zijn:

- Bankrekening- of creditcardgegevens (zoals rekeningnummer)
- Nationaal ID, zoals rijksregisternummer
- Paspoort nummer
- Salaris & gerelateerde vergoedingsinformatie
- Biometrische, gezondheids- en medische informatie
- Ras of etnische afstamming
- Politieke of religieuze overtuigingen
- Lidmaatschap van een vakbond

3.3 Wetten inzake gegevensbescherming

Veel landen hebben gegevensbeschermingswetgeving uitgevaardigd die voorwaarden opleggen voor de "verwerking" van persoonsgegevens. "Verwerking" kan onder andere acties omvatten zoals het verzamelen, gebruiken, opslaan, wijzigen, bekendmaken of doorgeven van persoonsgegevens. De verwerking van persoonsgegevens van EU-burgers (inclusief collega's en sollicitanten) is bijvoorbeeld zodanig geregeld dat elke verzameling, verwerking of overdracht van gegevens buiten de EU (of andere goedgekeurde staten) moet voldoen aan de wetgeving, zoals de Algemene Verordening Gegevensbescherming (AVG) van de EU.

Elke overdracht van EU persoonsgegevens buiten de EU - waaronder toegang tot EU persoonsgegevens van buiten de EU - vereist passende beveiligingsmaatregelen voorafgaand aan de gegevensoverdracht. Daarnaast vereist het delen van EU persoonsgegevens met een derde partij (zelfs met die partijen waarmee we een contract hebben) buiten de EU passende beveiliging en moet dit worden gecoördineerd met de juridische afdeling en het hoofd Ethics & Compliance.

3.4 – Uw verantwoordelijkheden om de Persoonsgegevens van Collega's te beschermen

Collega's en contractanten zijn verplicht om alle aspecten van dit Beleid die op hen van toepassing zijn, na te leven. Als u toegang hebt tot Persoonsgegevens en/of Gevoelige Persoonsgegevens, of gegevens van andere individuen op basis van uw rol binnen de onderneming, is het uw plicht om door Energizer goedgekeurde controles te implementeren om die gegevens te beveiligen en te beschermen en de toegang tot de gegevens te beperken tot alleen diegenen met een noodzaak om het te weten en alleen voor noodzakelijke en legitieme zakelijke doeleinden.

Energizer stelt de volgende richtlijnen op voor Medewerkers die bestanden met Persoonsgegevens of Gevoelige Persoonsgegevens openen, opslaan en/of verzenden (d.w.z. verwerken):

- i. Markeer alle documenten, bestanden of e-mails die Gevoelige Persoonsgegevens bevatten opvallend met de volgende markering:

"Persoonlijk en Vertrouwelijk"

- ii. Bestanden met dit soort gegevens mogen alleen worden opgeslagen op een beveiligde locatie zoals OneDrive, maar mogen **tijdelijk** worden opgeslagen op beveiligde bedrijfsbronnen zoals laptop- of desktopcomputers, om uiteindelijk te worden opgeslagen in OneDrive.
- iii. Bescherm bestanden met Gevoelige Persoonsgegevens met encryptie en/of wachtwoorden. Bestanden met Gevoelige Persoonsgegevens mogen alleen worden verzonden via beveiligde/gecodeerde methodes, zoals Subject Line Encryption, Citrix ShareFile of beveiligde verzendportalen met een leverancier.
- iv. Voordat u EU Persoonsgegevens en Gevoelige Persoonsgegevens met derden deelt, moet u ervoor zorgen dat dit zowel gepast als noodzakelijk is en contact opnemen met de onderstaande Privacyverantwoordelijken om ervoor te zorgen dat de juiste voorzorgsmaatregelen zijn genomen. Vergeet niet om uw computer te vergrendelen als u er even niet bent.
- v. Vergeet niet om uw computer te vergrendelen als u er afstand van moet nemen.
- vi. Laat uw laptop niet in het zicht of onbeveiligd achter in uw auto of hotelkamer en laat deze niet achter op een openbare locatie zoals een luchthaven.
- vii. Wees u ervan bewust dat zelfs gegevens zoals namen, e-mailadressen en andere informatie die betrekking hebben op een geïdentificeerde of identificeerbare persoon, onder de privacywetten van veel landen als "Persoonsgegevens" kunnen worden beschouwd en extra bescherming kunnen vereisen.
- viii. Gegevens moeten van uw computer worden verwijderd zodra u er niet langer toegang toe hoeft te hebben, tenzij ze onder een geschillenregeling of een ander bewaarschema vallen.

Ten slotte dient u het hoofd Ethics & Compliance op de hoogte te stellen als u niet zeker weet of bepaalde informatie of bestanden met een andere partij gedeeld mogen worden, als u zich bewust wordt van gevoelige informatie die per ongeluk of ongeoorloofd gedeeld is, of als uw laptop of mobiele apparaat (telefoon of tablet) verloren, gestolen of gecompromitteerd is. Gestolen laptops of mobiele apparaten moeten ook gemeld worden bij IT.

Deel 4: Bescherming van Vertrouwelijke en Bedrijfseigen Gegevens

Energizer Vertrouwelijke Gegevens

Vertrouwelijke informatie is informatie die schade kan toebrengen aan Energizer, haar klanten, collega's, of andere entiteiten of personen als deze ongepast openbaar wordt gemaakt, of informatie die anders niet publiekelijk beschikbaar is. Schade kan betrekking hebben op de privacy van een individu, de strategische zakelijke positie van Energizer of die van haar klanten, of wettelijke of toezichtsrechtelijke aansprakelijkheden. In overeenstemming met uw rollen en verantwoordelijkheden, kunt u toegang hebben tot Vertrouwelijke Gegevens van Energizer.

Voorbeelden van Vertrouwelijke Gegevens zijn strategische plannen, marketingplannen, financiële gegevens, klantenlijsten, contracten, bedrijfsplannen, niet-gepubliceerde octrooien, handelsgeheimen, documentatie over fusies en overnames, informatie die onderworpen is aan een geheimhoudingsovereenkomst of andere technische of zakelijke informatie.

Dit Beleid vereist de bescherming van Vertrouwelijke Gegevens bij het opslaan, verspreiden en delen zowel binnen als buiten de onderneming door gebruik te maken van geschikte administratieve, fysieke en technische beveiligingen in overeenstemming met de risico's die de mogelijke onbevoegde toegang tot de gegevens met zich meebrengt.

4.1 Uw verantwoordelijkheden om gegevens te beschermen

Tenzij het anders gemarkeerd is of duidelijk bedoeld is als Openbare Informatie, behandelt u alle informatie/gegevens alsof het Vertrouwelijke Gegevens van Energizer zijn, ongeacht de bron of vorm, inclusief elektronische, papieren, mondelinge of andere informatie.

Energizer stelt de volgende richtlijnen op voor het openen, opslaan en/of verzenden (d.w.z. verwerken) van bestanden die Energizer Vertrouwelijke Gegevens bevatten:

- Markeer opvallend alle documenten, bestanden of e-mails die Vertrouwelijke Gegevens van Energizer bevatten met het volgende:

"Energizer Bedrijfseigen en Vertrouwelijk"

- Bestanden met dit soort gegevens mogen alleen worden opgeslagen op een beveiligde locatie zoals OneDrive, maar mogen tijdelijk worden opgeslagen op beveiligde ondernemings-middelen zoals laptop- of desktopcomputers, om uiteindelijk te worden opgeslagen in OneDrive.
- Bescherm Vertrouwelijke Gegevens met de juiste versleuteling en/of wachtwoorden en verzend deze alleen via veilige methoden, zoals Subject Line Encryption, Citrix ShareFile of beveiligde verzendportalen.

- Vergeet niet om uw computer te vergrendelen als u er even niet bent.
- Laat uw laptop niet in het zicht of onbeveiligd achter in uw auto of hotelkamer en laat deze niet achter op een openbare locatie zoals een luchthaven.
- Vertrouwelijke gegevens moeten van uw computer worden verwijderd zodra u er niet langer toegang toe hoeft te hebben, tenzij ze onderhevig zijn aan geschillen of om te voldoen aan Energizer's schema voor het bewaren van gegevens.
- Bespreek Vertrouwelijke Gegevens alleen op niet-openbare plaatsen of door redelijke stappen te ondernemen om te voorkomen dat u gehoord wordt.
- Vertrouwelijke gegevens mogen alleen worden gescand, verspreid, gekopieerd en gedistribueerd voor zover dit noodzakelijk is, en ervoor zorgen dat de ontvangende partij onderworpen is aan een geheimhoudingsovereenkomst of soortgelijke geheimhoudingsverplichtingen.

Geef alle Vertrouwelijke Gegevens die in uw bezit zijn terug aan het einde van uw dienstverband en vergeet niet dat uw verplichting om vertrouwelijke gegevens te beschermen ook na beëindiging van het dienstverband blijft bestaan. **Als u zich ervan bewust wordt dat Vertrouwelijke Gegevens (opzettelijk of onopzettelijk) gedeeld zijn met onbevoegde partijen, of als uw laptop of mobiele apparaat verloren, gestolen of in gevaar gebracht is en Vertrouwelijke Gegevens bevat, neem dan onmiddellijk contact op met het Head of Ethics & Compliance en IT om het incident te melden.**

Hebt u een vraag of een probleem?

Er zijn veel manieren om een vraag te stellen of een probleem met betrekking tot dit Beleid te melden. Kies de optie die u het prettigst vindt om te gebruiken. Welke optie u ook kiest, uw vertrouwelijkheid zal worden gerespecteerd en vergelding zal niet worden getolereerd:

- Uw manager of leidinggevende
- Human Resources
- Ethics & Compliance energizercompliance@energizer.com
- Legal
- Energizer HelpLine: www.EnergizerHelpLine.com o Bel 0800 260 39 (BE)
 - Andere telefoonnummers www.EnergizerHelpLine.com
 - o SMS "Report" naar 314-668-1383 (enkel voor Noord-Amerika)
 - o U kunt anoniem blijven als u dat wilt
 - o 24 uur beschikbaar en beheerd door een externe provider

Deel 5: Verwante beleidslijnen en normen

Naam beleid[Code of Conduct](#)[Information Technology Acceptable Use Policy](#)[Records and Information Management \(RIM\) Policy](#)

Deel 6: Herzieningsgeschiedenis

De eigenaar van het beleid zal dit beleid ten minste eenmaal per boekjaar herzien en waar nodig bijwerken.

Revision Number	Effective Date	Owner	Description of Change
4	April 2024	Seth Smoker	Beleids eigenaar bijgewerkt; 'hoofd ethiek en naleving' gewijzigd in 'Algemene Raad van medewerkers, Global Ethics & Compliance' en contactinformatie gewijzigd in Karen Benson
3	Maart 2021	Ronnie Kann	Bijgewerkte contactgegevens voor Energizer HelpLine
2	Novemb 2020	Ronnie Kann	Beleidsverantwoordelijke bijgewerkt; "chief compliance officer" gewijzigd in "head of ethics & compliance"; toegevoegd hoe een vraag te stellen of een probleem te melden; RIM-beleid en Gedragscode toegevoegd aan verwant beleid en normen
1	Januari 2018	Kathy Rehmer	Nieuw beleid

Deel 7: Required Approval

Handtekening in dossier_____

Handtekening in dossier_____



Politique globale de protection des données

Date d'entrée en vigueur : février 2018

Dernière révision : avril 2025

Section 1: Objet de la présente politique

La présente Politique mondiale de protection des données (la « Politique ») favorise un équilibre efficace entre les pratiques de sécurité de l'information et les besoins commerciaux, tout en maintenant la conformité aux lois pertinentes. La politique aide Energizer à respecter nos obligations juridiques tout en maintenant la capacité de l'entreprise à être agile et à répondre aux attentes des clients. Comme il est décrit plus en détail ci-dessous, Energizer exige différents niveaux de contrôles de sécurité selon la classification des renseignements à protéger, lesquels sont fondés sur le risque, la commodité et d'autres considérations.

Nos clients, collègues et autres comptent sur nous pour protéger leurs renseignements. Une atteinte à la sécurité des données pourrait gravement nuire à notre crédibilité, causer la perte d'affaires et d'autres dommages aux personnes touchées. La sécurité solide des données exige la diligence de tous les collègues, entrepreneurs et autres personnes qui accèdent à nos données ou les utilisent. La protection des données fait partie du travail de tous.

Principes directeurs

Tous les collègues doivent garder à l'esprit les principes suivants en matière de protection des données :

- i. Energizer protège la confidentialité, l'intégrité et l'accès à ses données.
- ii. Energizer se conformera aux lois applicables en matière de confidentialité des données et de protection des données.
- iii. Energizer équilibre les besoins en efficacité commerciale avec le besoin de protéger les renseignements personnels, exclusifs et autres confidentiels contre les risques inutiles.
- iv. Energizer ne donne accès qu'à des renseignements personnels, exclusifs et confidentiels aux personnes qui ont besoin de les connaître et qui sont tenues de maintenir la sécurité de ces renseignements.
- v. Les collègues d'Energizer constituent la première et la meilleure ligne de défense contre les incidents de sécurité des données, et il incombe à chaque collègue de respecter les pratiques de cette politique.
- vi. Le réseau, les systèmes et les autres actifs d'Energizer sont principalement utilisés à des fins commerciales. Sauf si la loi applicable le prévoit autrement, vous ne devez pas vous attendre à la confidentialité lorsque vous utilisez le réseau ou les systèmes d'Energizer, y compris, mais sans s'y limiter, la transmission et le stockage de fichiers, de données et de messages.

Section 2: Responsable de la politique et déclaration de responsabilité

Cette politique est la responsabilité de l'avocat-conseil adjoint, Éthique et conformité à l'échelle mondiale. Il incombe à cette personne, ainsi qu'au Service juridique, de mettre en œuvre, de réviser annuellement et de réviser cette politique au besoin.



Politique globale de protection des données

Date d'entrée en vigueur : février 2018

Dernière révision : avril 2025

Nom	Titre	Téléphone	Courriel
Karen Benson	Chef adjoint du contentieux, Éthique mondiale et conformité	954.593.6876	karen.benson@energizer.com

Section 3: Protection des données personnelles

3.1 Collecte et traitement des données des collègues

Afin de gérer efficacement son entreprise, Energizer doit recueillir et utiliser certains renseignements personnels sur ses collègues. Les lois et règlements mondiaux sur la confidentialité des données exigent la collecte, le stockage, le traitement, le partage, le transfert et l'utilisation appropriés des données personnelles, y compris les données personnelles des collègues (« Données personnelles des collègues »). Il incombe aux collègues, tel que décrit dans le Code de conduite, d'utiliser les données uniquement aux fins prévues et de les protéger de façon appropriée.

Certaines données, y compris les données personnelles sensibles et les données personnelles, sont recueillies auprès des collègues – et dans certains cas des candidats à un emploi – soit par des tiers autorisés de l'entreprise ou de l'entreprise pour administrer tous les aspects de l'emploi, y compris, mais sans s'y limiter : paie, rémunération, déplacements, remboursement des dépenses, don en ligne, administration des avantages sociaux, procédures disciplinaires et griefs, temps et présence, gestion des cours de formation et gestion de carrière.

Lorsque cela est nécessaire à des fins professionnelles et permis par la loi, Energizer peut aussi accéder aux courriels et aux documents, y compris les curriculum vitæ (CV), qui peuvent contenir des données personnelles ou sensibles, et les stocker. Energizer peut également recueillir des données sur les collègues lorsqu'il surveille les communications et les systèmes afin de protéger l'entreprise contre les virus et les logiciels malveillants ou pour assurer la conformité aux politiques, aux lois et aux règlements.

3.2 Types de données collectées sur les collègues

3.2(a) – Données personnelles

Dans l'Union européenne (UE) et dans de nombreux autres pays, les « données personnelles » sont définies de façon générale comme toute information relative à une personne identifiée ou identifiable (c.-à-d. une personne qui peut être identifiée directement ou indirectement par référence à un nom, un numéro d'identification, etc.). En termes simples, les données personnelles peuvent inclure le nom, l'adresse électronique, l'adresse physique ou autre d'une personne.

3.2(b) – Données personnelles sensibles

Les lois sur la confidentialité des données varient d'un pays à l'autre et certains éléments de données sont considérés comme sensibles dans certaines juridictions et nécessitent une protection supplémentaire, car l'utilisation inappropriée de ces données peut mener au vol d'identité. Par exemple, les données personnelles sensibles peuvent comprendre :

- Renseignements sur le compte bancaire ou la carte de crédit (comme le numéro de compte et le numéro d'acheminement)
- Code d'identification national, comme le numéro d'assurance sociale
- Numéro de passeport
- Renseignements sur le salaire et la rémunération connexes
- Renseignements biométriques, sur la santé et médicaux
- Origine raciale ou ethnique
- Croyances politiques ou religieuses
- Adhésion syndicale

3.3 Lois sur la protection des données

De nombreux pays ont promulgué des lois sur la confidentialité des données qui précisent des exigences pour le "traitement" des données personnelles. « Traitement » peut comprendre des actions telles que la collecte, l'utilisation, le stockage, la modification, la divulgation, ou la transmission de données personnelles, entre autres. Par exemple, le traitement des données personnelles des citoyens de l'UE (y compris les collègues et les demandeurs) est réglementé de façon à ce que toute collecte, tout traitement ou tout transfert de données à l'extérieur de l'UE (ou d'autres États approuvés) soit conforme aux lois, telles que le Règlement général sur la protection des données (RGPD) de l'UE.

Tout transfert de données personnelles de l'UE à l'extérieur de l'UE -- qui inclut l'accès aux données personnelles de l'UE depuis l'extérieur de l'UE -- nécessite des mesures de protection appropriées avant le transfert des données. De plus, le partage des données personnelles de l'UE avec un tiers (même avec ceux avec qui nous avons un contrat) à l'extérieur de l'UE exige une sécurité appropriée et doit être coordonné avec le Service juridique et le chef de l'éthique et de la conformité.

3.4 – Vos responsabilités en matière de protection des données des collègues

Les collègues et les entrepreneurs sont tenus de se conformer à tous les aspects de la présente politique qui s'appliquent à eux. Si vous avez accès à des données personnelles ou sensibles ou à d'autres données individuelles en fonction de votre rôle au sein de l'entreprise, il vous incombe de mettre en œuvre des contrôles approuvés par Energizer pour sécuriser et protéger ces données et limiter l'accès aux données uniquement aux personnes qui en ont besoin et uniquement aux fins commerciales nécessaires et légitimes.

Energizer établit les lignes directrices suivantes pour les collègues qui accèdent, enregistrent ou transmettent (c.-à-d., traitent) des fichiers contenant des données personnelles ou des données personnelles sensibles :

- i. Marquez bien en évidence tous les documents, fichiers ou courriels qui contiennent des données personnelles sensibles avec le marquage suivant :

« Personnel et confidentiel »

- ii. Les fichiers contenant ce type de données ne doivent être sauvegardés que dans un endroit sécurisé comme OneDrive, mais ils peuvent être stockés **temporairement** sur des ressources sécurisées de l'entreprise, comme un ordinateur portable ou un ordinateur de bureau, et éventuellement stockés dans OneDrive.
- iii. Protégez les fichiers de données personnelles sensibles avec le chiffrement ou les mots de passe. Les fichiers de données personnelles sensibles ne doivent être transmis que par des méthodes sécurisées/cryptées, comme le chiffrement de la ligne d'objet, Citrix ShareFile ou des portails de transmission sécurisés avec un fournisseur.
- iv. Avant de partager les données personnelles et les données personnelles sensibles de l'UE avec des tiers, assurez-vous qu'elles sont appropriées et nécessaires et communiquez avec les ressources en matière de protection des renseignements personnels ci-dessous pour assurer la mise en place de mesures de protection appropriées.
- v. N'oubliez pas de verrouiller votre ordinateur si vous devez vous éloigner de celui-ci.
- vi. Ne laissez pas votre ordinateur portable à la vue, ou non sécurisé, dans votre voiture ou dans une chambre d'hôtel, et ne vous éloignez pas de celui-ci dans un endroit public comme un aéroport.
- vii. Sachez que même des données telles que les noms, adresses électroniques et autres renseignements liés à une personne identifiée ou identifiable peuvent être considérées comme des « données personnelles » en vertu des lois sur la protection de la vie privée de nombreux pays et peuvent nécessiter des protections supplémentaires.
- viii. Les données doivent être supprimées de votre ordinateur dès que vous n'avez plus besoin d'y accéder, sauf si elles font l'objet d'un litige ou d'un autre calendrier de conservation des documents.

Enfin, avisez le chef de l'éthique et de la conformité si vous n'êtes pas certain si certains renseignements ou fichiers peuvent être partagés avec une autre partie, si vous prenez connaissance de renseignements sensibles partagés par erreur ou non autorisés, ou si votre portable ou appareil mobile (téléphone ou tablette) a été perdu, volé ou compromis. Les ordinateurs portatifs ou les appareils mobiles volés doivent également être signalés au service de conciergerie des TI.

Section 4: Protection des données confidentielles ou exclusives de l'entreprise

Données confidentielles d'Energizer

Les renseignements confidentiels sont des renseignements qui peuvent causer du tort à Energizer, à ses clients, à ses collègues ou à d'autres entités ou personnes s'ils sont divulgués de façon inappropriée, ou des renseignements qui ne sont pas autrement accessibles au public. Les risques peuvent être liés à la vie privée d'une personne, à la position commerciale stratégique d'Energizer ou à celle de ses clients, ou à des responsabilités juridiques ou réglementaires. Conformément à vos rôles et responsabilités, vous pouvez avoir accès aux données confidentielles d'Energizer.

Des exemples de données confidentielles comprennent les plans stratégiques, les plans de marketing, les données financières, les listes de clients, les contrats, les plans d'affaires, les brevets non publiés, les secrets commerciaux, la documentation sur les fusions et Acquisitions, les renseignements assujettis à une entente de non-divulgence ou toute autre information technique ou commerciale.

La présente politique exige la protection des données confidentielles dans le stockage, la diffusion et le partage, tant à l'intérieur qu'à l'extérieur de l'entreprise, au moyen de mesures de protection administratives, physiques et techniques appropriées, en fonction des risques que pose l'accès non autorisé possible aux données.

4.1 Vos responsabilités en matière de protection des données de l'entreprise

À moins qu'elles ne soient marquées autrement ou qu'elles ne soient clairement destinées à être des renseignements publics, traiter toute information ou donnée comme s'il s'agissait de données confidentielles d'Energizer, quelle que soit leur source ou leur forme, y compris les renseignements électroniques, papier, verbaux ou autres.

Energizer établit les directives suivantes pour accéder aux fichiers contenant des données confidentielles d'Energizer, les sauvegarder ou les transmettre (c.-à-d., les traiter) :

- Marquez bien en évidence tous les documents, fichiers ou courriels contenant des données confidentielles d'Energizer avec les éléments suivants :

« Energizer Proprietary and Confidential »

- Les fichiers contenant ce type de données ne doivent être sauvegardés que dans un endroit sécurisé comme OneDrive, mais ils peuvent être stockés temporairement sur des ressources sécurisées de l'entreprise, comme un ordinateur portable ou un ordinateur de bureau, et éventuellement stockés dans OneDrive.
- Protégez les données confidentielles à l'aide d'un cryptage ou d'un mot de passe appropriés et transmettez-les uniquement en utilisant des méthodes sécurisées,



Politique globale de protection des données

Date d'entrée en vigueur : février 2018

Dernière révision : avril 2025

comme le chiffrement de la ligne d'objet, Citrix ShareFile ou des portails de transmission sécurisés.

- N'oubliez pas de verrouiller votre ordinateur si vous devez vous éloigner de celui-ci.
- Ne laissez pas votre ordinateur portatif à la vue, ou non sécurisé, dans votre voiture ou dans une chambre d'hôtel, et ne vous éloignez pas de celui-ci dans un endroit public comme un aéroport.
- Les données confidentielles doivent être supprimées de votre ordinateur dès que vous n'avez plus besoin d'y accéder, à moins qu'elles ne soient assujetties à une mise en suspens pour litige ou à d'autres raisons afin de respecter le calendrier de conservation des documents d'Energizer.
- Ne discutez des données confidentielles que dans des endroits non publics ou en prenant des mesures raisonnables pour éviter d'être entendus.
- Numérisez, distribuez, copiez et distribuez les données confidentielles uniquement dans la mesure nécessaire, et assurez-vous que la partie réceptrice est assujettie à une entente de confidentialité ou à des obligations similaires de confidentialité.

Retournez toutes les données confidentielles que vous avez en votre possession à la fin de votre emploi et rappelez-vous que votre obligation de protéger les données confidentielles survivra à la fin de votre emploi. **Si vous apprenez que des données confidentielles ont été partagées avec des tiers non autorisés (intentionnellement ou non), ou que votre ordinateur portatif ou appareil mobile a été perdu, volé ou compromis et qu'il contenait des données confidentielles, veuillez communiquer immédiatement avec le chef de l'éthique et de la conformité et avec le concierge informatique pour signaler l'incident.**

Vous avez une question ou une préoccupation?

Il existe de nombreuses façons de poser une question ou de soulever une préoccupation concernant cette politique. Choisissez l'option qui vous convient le mieux. Quelle que soit l'option que vous choisirez, votre confidentialité sera respectée et les représailles ne seront pas tolérées :

- Votre directeur ou votre supérieur immédiat
- Ressources humaines
- Éthique et conformité energizercompliance@energizer.com
- Juridique
- Ligne d'assistance Energizer : www.EnergizerHelpLine.com
 - Composez le 1-877-521-5625 (É.-U.)
 - Numéros de téléphone supplémentaires à www.EnergizerHelpLine.com
 - Texte « Rapport » au 314-668-1383 (Amérique du Nord seulement)
 - vous pouvez demeurer anonyme si vous le souhaitez
 - disponible 24 heures et exploité par un fournisseur de 3e partie



Politique globale de protection des données

Date d'entrée en vigueur : février 2018

Dernière révision : avril 2025

Section 5: Politiques et normes connexes

Nom de la politique
Code de conduite
Politique d'utilisation acceptable des technologies de l'information
Politique de gestion des documents et de l'information (RIM)

Section 6: Historique des révisions

Le responsable de la police examinera et mettra à jour la présente politique au besoin au moins une fois par exercice financier.

Numéro de révision	Date d'entrée en vigueur	Propriétaire	Description du changement
4	Avril 2024	Seth Smoker	Responsable de la politique mis à jour; « chef de l'éthique et de la conformité » remplacé par « avocate générale associée, Éthique et conformité à l'échelle mondiale » et coordonnées modifiées par Karen Benson
3	Mars 2021	Ronnie Kann	Mise à jour des coordonnées de la ligne d'assistance Energizer
2	Novembre 2020	Ronnie Kann	Responsable de la politique mis à jour; « chef de la conformité » remplacé par « chef de l'éthique et de la conformité »; ajout de la façon de poser une question ou de soulever une préoccupation; ajout de la politique et du code de conduite de la Gestion des documents et de l'information aux politiques et aux normes connexes
1	Janvier 2018	Kathy Rehmer	Nouvelle politique

Section 7: Approbation requise

Signature au dossier _____

Signature au dossier _____



Politique mondiale de protection des données

Date d'entrée en vigueur : février 2018

Dernière révision : avril 2025

Section 1: Objet de la présente politique

Cette politique mondiale de protection des données (la « politique ») favorise un équilibre efficace entre les pratiques de sécurité des informations et les besoins de l'entreprise, tout en maintenant la conformité avec les lois applicables. La politique aide Energizer à respecter ses obligations légales tout en maintenant la capacité de l'entreprise à être agile et à répondre aux attentes des clients. Comme indiqué ci-dessous plus en détail, Energizer exige différents niveaux de contrôles de sécurité en fonction de la classification des renseignements à protéger, lesquels sont basés sur le risque, la praticité et d'autres considérations.

Nos clients, collègues et autres comptent sur nous pour protéger leurs informations. Une violation de la sécurité des données pourrait gravement nuire à notre crédibilité, causer des pertes d'activité et d'autres préjudices aux personnes affectées. Une sécurité renforcée des données exige la diligence de tous les collègues, sous-traitants et autres personnes accédant à nos actifs de données ou les utilisant. La protection des données fait partie du travail de chacun.

Principes directeurs

Tous les collaborateurs doivent garder à l'esprit les principes suivants en matière de protection des données :

- i. Energizer protège la confidentialité, l'intégrité et l'accès à ses actifs de données.
- ii. Energizer se conformera aux lois applicables en matière de confidentialité et de protection des données.
- iii. Energizer équilibre les besoins d'efficacité de l'entreprise avec la nécessité de protéger les informations personnelles, exclusives et autres informations confidentielles contre les risques inutiles.
- iv. Energizer n'accorde l'accès aux renseignements personnels, exclusifs et autres renseignements confidentiels qu'à ceux qui ont besoin de les connaître et qui sont tenus de maintenir la sécurité des renseignements.
- v. Les employés d'Energizer sont la première et la meilleure ligne de défense contre les incidents de sécurité des données, et il est de la responsabilité de chaque employé de respecter les pratiques de la présente politique.
- vi. Le réseau, les systèmes et les autres actifs d'Energizer sont principalement destinés à des fins commerciales. Sauf disposition contraire de la loi applicable, vous ne devriez avoir aucune attente en matière de confidentialité lorsque vous utilisez le réseau ou les systèmes d'Energizer, y compris, mais sans s'y limiter, la transmission et le stockage de fichiers, de données et de messages.

Section 2: Propriétaire de la police et Déclaration de responsabilité

Cette politique est la propriété de l'avocat général associé, Global Ethics & Compliance. Il incombe à cette personne, de concert avec le Service juridique, de mettre en œuvre, d'examiner chaque année et de réviser cette politique au besoin.



Politique mondiale de protection des données

Date d'entrée en vigueur : février 2018

Dernière révision : avril 2025

Nom	Titre	Téléphone	E-mail
Karen Benson	Avocat-conseil associé, Global Ethics & Compliance	954.593.6876	karen.benson@energizer.com

Section 3: Protection des données personnelles

3.1 Collecte et traitement des données des employés

Afin de mener efficacement ses activités, Energizer doit recueillir et utiliser certains renseignements personnels sur ses collègues. Les lois et réglementations mondiales en matière de confidentialité des données exigent la collecte, le stockage, le traitement, le partage, le transfert et l'utilisation appropriés des données personnelles, y compris les données personnelles des collègues (« données personnelles des collègues »). Il est de la responsabilité fondamentale des collègues, comme le prévoit le Code de conduite, de n'utiliser les données qu'aux fins prévues et de les protéger de manière appropriée.

Certaines données, y compris les données personnelles sensibles et les données personnelles, sont collectées auprès de collègues -- et dans certains cas des candidats à un emploi -- soit par la société ou des tiers autorisés de la société à administrer tous les aspects de l'emploi, y compris, mais sans s'y limiter : paie, rémunération, voyages, remboursement de dépenses, dons en ligne, administration des avantages sociaux, procédures disciplinaires et de règlement des griefs, temps et présence, gestion des cours de formation et gestion de carrière.

Lorsque cela est nécessaire à des fins commerciales et autorisé par la loi, Energizer peut également accéder et stocker des courriels et des documents, y compris des CV, qui peuvent contenir des données personnelles ou sensibles. Energizer peut également recueillir des données sur les employés lorsqu'elle surveille les communications et les systèmes afin de protéger l'entreprise contre les virus et les logiciels malveillants ou pour assurer la conformité aux politiques, lois et règlements.

3.2 Types de données recueillies sur les employés

3.2(a) – Données personnelles

Dans l'Union européenne (UE) et dans de nombreux autres pays, les « données personnelles » sont définies au sens large comme toute information relative à une personne identifiée ou identifiable (c'est-à-dire une personne qui peut être identifiée directement ou indirectement par référence à un nom, un numéro d'identification, etc.). En termes simples, les données personnelles peuvent inclure le nom d'une personne, son adresse e-mail, son adresse physique ou autre.

3.2(b) – Données personnelles sensibles

Les lois sur la confidentialité des données varient selon les pays et certains éléments de données sont considérés comme sensibles dans certaines juridictions et nécessitent une protection supplémentaire car une utilisation inappropriée de ces données peut entraîner un vol d'identité. Par exemple, les données personnelles sensibles peuvent inclure :

- Informations relatives au compte bancaire ou à la carte de crédit (telles que le numéro de compte et le numéro de routage)
- ID national, tel que le numéro de sécurité sociale
- Passeport no
- Informations sur le salaire et la rémunération associée
- Informations biométriques, sanitaires et médicales
- Origine raciale ou ethnique
- Croyances politiques ou religieuses
- Adhésion syndicale

3.3 Lois sur la protection des données

De nombreux pays ont promulgué des lois sur la confidentialité des données qui spécifient les exigences pour le « traitement » des données personnelles. Le « traitement » peut inclure des actions telles que la collecte, l'utilisation, le stockage, la modification, la divulgation, ou transmettre des données personnelles, entre autres. Par exemple, le traitement des données personnelles des citoyens de l'UE (y compris les collègues et les candidats) est réglementé de sorte que toute collecte, traitement ou transfert de données en dehors de l'UE (ou d'autres états approuvés) doit être conforme aux lois, telles que le Règlement général sur la protection des données (RGPD) de l'UE.

Tout transfert de données personnelles de l'UE en dehors de l'UE - ce qui inclut l'accès aux données personnelles de l'UE depuis l'extérieur de l'UE - nécessite des garanties appropriées avant le transfert de données. En outre, le partage de données personnelles de l'UE avec un tiers (même avec qui nous avons un contrat) en dehors de l'UE nécessite une sécurité appropriée et doit être coordonné avec le Service juridique et le responsable éthique et conformité.

3.4 – Vos responsabilités en matière de protection des données de vos collègues

Les employés et les sous-traitants sont tenus de se conformer à tous les aspects de la présente politique qui s'appliquent à eux. Si vous avez accès à des données personnelles et/ou à des données personnelles sensibles, ou à des données d'autres personnes en fonction de votre rôle au sein de la Société, il est de votre devoir de mettre en œuvre des contrôles approuvés par Energizer pour sécuriser et protéger ces données et limiter l'accès aux données uniquement à ceux qui en ont besoin et uniquement à des fins commerciales nécessaires et légitimes.



Politique mondiale de protection des données

Date d'entrée en vigueur : février 2018

Dernière révision : avril 2025

Energizer énonce les directives suivantes pour les employés qui accèdent, enregistrent et/ou transmettent (c.-à-d. traitent) des fichiers contenant des données personnelles ou des données personnelles sensibles :

- i. Marquez bien en évidence tous les documents, fichiers ou e-mails qui contiennent des données personnelles sensibles avec le marquage suivant :

« Personnel et confidentiel »

- ii. Les fichiers contenant ce type de données ne doivent être enregistrés que dans un emplacement sécurisé tel que OneDrive, mais peuvent être stockés **temporairement** sur des ressources sécurisées de l'entreprise telles que des ordinateurs portables ou de bureau, pour éventuellement être stockés dans OneDrive.
- iii. Protégez les fichiers de données personnelles sensibles avec un cryptage et/ou des mots de passe. Les fichiers de données personnelles sensibles ne doivent être transmis qu'à l'aide de méthodes sécurisées/cryptées, telles que le chiffrement de ligne d'objet, Citrix ShareFile ou des portails de transmission sécurisés avec un fournisseur.
- iv. Avant de partager des données personnelles de l'UE et des données personnelles sensibles avec des tiers, assurez-vous que cela est à la fois approprié et nécessaire et contactez les ressources de confidentialité ci-dessous pour vous assurer que les mesures de protection appropriées sont en place.
- v. N'oubliez pas de verrouiller votre ordinateur si vous devez vous en éloigner.
- vi. Ne laissez pas votre ordinateur portable à la vue, ou non sécurisé, dans votre voiture ou une chambre d'hôtel et ne vous éloignez pas de lui dans un lieu public tel qu'un aéroport.
- vii. Sachez que même les données telles que les noms, adresses e-mail et autres informations relatives à une personne identifiée ou identifiable peuvent être considérées comme des « données personnelles » en vertu des lois sur la confidentialité de nombreux pays et peuvent nécessiter des protections supplémentaires.
- viii. Les données doivent être supprimées de votre ordinateur dès que vous n'avez plus besoin d'y accéder, sauf si elles font l'objet d'une suspension pour litige ou d'un autre calendrier de conservation des documents.

Enfin, informez le responsable de l'éthique et de la conformité si vous n'êtes pas sûr que certaines informations ou certains fichiers peuvent être partagés avec une autre partie, si vous avez connaissance d'informations sensibles qui ont été partagées par erreur ou non, ou si votre ordinateur portable ou votre appareil mobile (téléphone ou tablette) a été perdu, volé ou compromis. Les ordinateurs portables ou les appareils mobiles volés doivent également être signalés au service de conciergerie INFORMATIQUE.

Section 4: Protection des données confidentielles ou propriétaires de l'entreprise

Données confidentielles Energizer

Les informations confidentielles sont des informations qui peuvent causer un préjudice à Energizer, ses clients, collègues ou autres entités ou individus si elles sont divulguées de manière inappropriée, ou des informations qui ne sont pas autrement accessibles au public. Les préjudices peuvent être liés à la vie privée d'une personne, à la position commerciale stratégique d'Energizer ou à celle de ses clients, ou à des responsabilités légales ou réglementaires. Conformément à vos rôles et responsabilités, vous pouvez avoir accès aux données confidentielles Energizer.

Exemples de données confidentielles : plans stratégiques, plans marketing, données financières, listes de clients, contrats, plans d'affaires, brevets non publiés, secrets commerciaux, documentation de fusions et Acquisitions, informations faisant l'objet d'un accord de non-divulgaration ou autres informations techniques ou commerciales.

Cette politique exige la protection des données confidentielles dans le stockage, la diffusion et le partage à l'intérieur et à l'extérieur de l'entreprise en utilisant des mesures de protection administratives, physiques et techniques appropriées en fonction des risques posés par l'accès non autorisé possible aux données.

4.1 Vos responsabilités en matière de protection des données de l'entreprise

Sauf indication contraire ou clairement destinée à être une information publique, traitez toutes les informations/données comme si elles étaient des données confidentielles, quelle que soit leur source ou leur forme, y compris les informations électroniques, papier, verbales ou autres.

Energizer énonce les directives suivantes pour accéder, sauvegarder et/ou transmettre (c.-à-d., traiter) les fichiers contenant des données confidentielles Energizer :

- Marquez bien en évidence tous les documents, fichiers ou courriels qui contiennent des données confidentielles Energizer avec les éléments suivants :

« Energizer propriétaire et confidentiel »

- Les fichiers contenant ce type de données ne doivent être enregistrés que dans un emplacement sécurisé tel que OneDrive, mais peuvent être stockés temporairement sur des ressources sécurisées de l'entreprise telles que des ordinateurs portables ou de bureau, pour éventuellement être stockés dans OneDrive.
- Protégez les données confidentielles avec un cryptage et/ou des mots de passe appropriés et transmettez-les uniquement à l'aide de méthodes sécurisées, telles que le cryptage par ligne d'objet, Citrix ShareFile ou des portails de transmission sécurisés.
- N'oubliez pas de verrouiller votre ordinateur si vous devez vous en éloigner.

Politique mondiale de protection des données

Date d'entrée en vigueur : février 2018

Dernière révision : avril 2025

- Ne laissez pas votre ordinateur portable à la vue, ou non sécurisé, dans votre voiture ou une chambre d'hôtel et ne vous éloignez pas de lui dans un lieu public tel qu'un aéroport.
- Les données confidentielles doivent être supprimées de votre ordinateur dès que vous n'avez plus besoin d'y accéder, sauf si elles font l'objet d'une suspension pour litige ou autre pour se conformer au calendrier de conservation des documents d'Energizer.
- Ne discutez des données confidentielles que dans des lieux non publics ou en prenant des mesures raisonnables pour éviter d'être entendues.
- Scannez, distribuez, copiez et distribuez uniquement les données confidentielles dans la mesure nécessaire, et assurez-vous que la partie destinataire est soumise à un accord de non-divulgaration ou à des obligations similaires de confidentialité.

Retournez toutes les données confidentielles en votre possession à la fin de votre emploi et rappelez-vous que votre obligation de protéger les données confidentielles survit après la cessation de votre emploi. **Si vous vous rendez compte que des données confidentielles ont été partagées avec des tiers non autorisés (intentionnellement ou non), ou que votre ordinateur portable ou votre appareil mobile a été perdu, volé ou compromis et qu'il contenait des données confidentielles, veuillez contacter immédiatement le responsable éthique et conformité et le concierge INFORMATIQUE pour signaler l'incident.**

Vous avez une question ou une préoccupation ?

Il existe de nombreuses façons de poser une question ou de soulever une préoccupation au sujet de cette politique. Choisissez l'option qui vous convient le mieux. Quelle que soit l'option choisie, votre confidentialité sera respectée et aucune représailles ne sera tolérée :

- Votre responsable ou votre supérieur hiérarchique
- Ressources humaines
- Éthique et conformité energizercompliance@energizer.com
- Juridique
- Ligne d'assistance Energizer : www.EnergizerHelpLine.com
 - Appelez le 1-877-521-5625 (États-Unis)
 - Numéros de téléphone supplémentaires au www.EnergizerHelpLine.com
 - Texte « Report » au 314-668-1383 (Amérique du Nord seulement)
 - vous pouvez rester anonyme si vous le souhaitez
 - disponible 24 heures sur 24 et exploité par un fournisseur tierces parties

Section 5: Politiques et normes connexes

Nom de la stratégie
Code de conduite
Politique d'utilisation acceptable des technologies de l'information



Politique mondiale de protection des données

Date d'entrée en vigueur : février 2018

Dernière révision : avril 2025

[Politique de gestion des documents et de l'information \(RIM\)](#)

Section 6: Historique des révisions

Le propriétaire de la police examinera et mettra à jour cette police au besoin au moins une fois par exercice.

Numéro de révision	Date d'entrée en vigueur	Propriétaire	Description de la modification
4	Avril 2024	Seth Smoker	Mise à jour du propriétaire de la politique ; changement de « responsable de l'éthique et de la conformité » en « avocat général associé, éthique mondiale et conformité » et changement des coordonnées en Karen Benson
3	Mars 2021	Ronnie Kann	Mise à jour des coordonnées de la ligne d'assistance d'Energizer
2	Novembre 2020	Ronnie Kann	Mise à jour du propriétaire de la politique ; modification de « Chief Compliance Officer » en « Head of Ethics & Compliance » ; ajout de la façon de poser une question ou de signaler un problème ; ajout de la politique RIM et du Code de conduite à la politique et aux normes connexes
1	Janvier 2018	Kathy Rehmer	Nouvelle politique

Section 7: Approbation requise

Signature sur dossier _____

Signature sur dossier _____

Section 1: Zweck dieser Richtlinie

Diese Globale Datenschutzrichtlinie (die „Richtlinie“) fördert ein effektives Gleichgewicht zwischen Verfahren zur Informationssicherheit und Geschäftsanforderungen bei gleichzeitiger Einhaltung der einschlägigen Gesetze. Die Richtlinie hilft Energizer dabei, unsere gesetzlichen Verpflichtungen zu erfüllen und gleichzeitig die Fähigkeit des Unternehmens zu erhalten, flexibel zu sein und Kundenerwartungen zu erfüllen. Wie im Folgenden näher ausgeführt, verlangt Energizer je nach Klassifizierung der zu schützenden Informationen unterschiedliche Sicherheitskontrollen, die auf Risiken, Praktikabilität und anderen Erwägungen basieren.

Unsere Kunden, Kollegen und andere verlassen sich beim Schutz ihrer Daten auf uns. Eine Datenschutzverletzung könnte unsere Glaubwürdigkeit erheblich beeinträchtigen, Geschäftsverluste und andere Schäden für betroffene Personen verursachen. Eine hohe Datensicherheit erfordert Sorgfalt von allen Kollegen, Auftragnehmern und anderen Personen, die auf unsere Datenbestände zugreifen oder diese nutzen. Datenschutz ist Teil der Arbeit aller.

Leitprinzipien

Alle Kollegen sollten die folgenden Datenschutzgrundsätze beachten:

- i. Energizer schützt die Vertraulichkeit, Integrität und den Zugriff auf seine Datenbestände.
- ii. Energizer wird die geltenden Datenschutzgesetze und Datenschutzgesetze einhalten.
- iii. Energizer gleicht die Anforderungen an Geschäftseffizienz mit der Notwendigkeit aus, persönliche, proprietäre und andere vertrauliche Informationen vor unnötigen Risiken zu schützen.
- iv. Energizer gewährt nur Personen Zugriff auf persönliche, proprietäre und andere vertrauliche Informationen, die Kenntnis benötigen und die zur Wahrung der Sicherheit der Informationen verpflichtet sind.
- v. Mitarbeiter von Energizer sind die erste und beste Verteidigungslinie gegen Datensicherheitsvorfälle, und es liegt in der Verantwortung jedes Mitarbeiters, die Praktiken dieser Richtlinie einzuhalten.
- vi. Energizers Netzwerk, Systeme und andere Vermögenswerte sind hauptsächlich für geschäftliche Zwecke bestimmt. Sofern das anwendbare Recht nichts anderes vorsieht, sollten Sie bei der Nutzung des Netzwerks oder der Systeme von Energizer keine Erwartungen an den Datenschutz haben, einschließlich aber nicht beschränkt auf die Übertragung und Speicherung von Dateien, Daten und Nachrichten.

Section 2: Verantwortlicher der Police und Erklärung der Verantwortung

Für diese Richtlinie ist der Associate General Counsel, Global Ethics & Compliance verantwortlich. Es liegt in der Verantwortung dieser Person, zusammen mit der Rechtsabteilung, diese Richtlinie bei Bedarf umzusetzen, jährlich zu überprüfen und zu überarbeiten.

Name	Titel	Telefon	E-Mail
Karen Benson	Associate General Counsel, Global Ethics & Compliance	954.593.6876	karen.benson@energizer.com

Section 3: Schutz Personenbezogener Daten

3.1 Erfassung und Verarbeitung von Mitarbeiterdaten

Um das Geschäft effektiv zu führen, muss Energizer bestimmte persönliche Daten über unsere Kollegen erfassen und nutzen. Globale Datenschutzgesetze und -Vorschriften verlangen eine angemessene Erfassung, Speicherung, Verarbeitung, Weitergabe, Übertragung und Nutzung personenbezogener Daten, einschließlich der personenbezogenen Daten von Kollegen („personenbezogene Daten von Kollegen“). Es liegt in der grundsätzlichen Verantwortung der Kollegen, wie im Verhaltenskodex dargelegt, die Daten nur für den vorgesehenen Zweck zu verwenden und diese Daten angemessen zu schützen.

Bestimmte Daten, einschließlich sensibler personenbezogener Daten und personenbezogener Daten, werden von Kollegen – und in einigen Fällen von Bewerbern für eine Beschäftigung – entweder von dem Unternehmen oder von autorisierten Dritten des Unternehmens erhoben, um alle Aspekte der Beschäftigung zu verwalten, einschließlich, aber nicht beschränkt auf: Gehaltsabrechnung, Entschädigung, Reise, Kostenerstattung, Online-Spenden, Leistungsverwaltung, Disziplinarverfahren und Beschwerdeverfahren, Zeit- und Anwesenheitszeiten, Schulungskursmanagement und Karrieremanagement.

Wenn dies für geschäftliche Zwecke erforderlich ist und gesetzlich zulässig ist, kann Energizer auch auf E-Mails und Dokumente zugreifen und diese speichern, einschließlich Lebensläufe (Lebensläufe), die personenbezogene oder sensible Daten enthalten können. Energizer kann auch Daten von Kollegen erfassen, wenn es Kommunikation und Systeme überwacht, um das Unternehmen vor Viren und Malware zu schützen oder um die Einhaltung von Richtlinien, Gesetzen und Vorschriften sicherzustellen.

3.2 Arten der erfassten Mitarbeiterdaten

3.2(a) – Personenbezogene Daten

In der Europäischen Union (EU) und in vielen anderen Ländern sind „personenbezogene Daten“ allgemein als alle Informationen definiert, die sich auf eine identifizierte oder identifizierbare Person beziehen (d. h. eine Person, die direkt oder indirekt anhand eines Namens, einer ID-Nummer usw. identifiziert werden kann). Einfach ausgedrückt: Persönliche Daten können den Namen, die E-Mail-Adresse, die physische Adresse oder ähnliches umfassen.

3.2(b) – Sensible Personenbezogene Daten

Die Datenschutzgesetze sind von Land zu Land unterschiedlich, und einige Datenelemente gelten in bestimmten Ländern als sensibel und erfordern zusätzlichen Schutz, da eine unsachgemäße Verwendung dieser Daten zu Identitätsdiebstahl führen kann. Sensible personenbezogene Daten können beispielsweise Folgendes umfassen:

- Bankkonto- oder Kreditkarteninformationen (z. B. Kontonummer und Bankleitzahl)
- Nationale ID, z.B. Sozialversicherungsnummer
- Reisepassnummer
- Gehaltsinformationen und zugehörige Vergütungsinformationen
- Biometrische, gesundheitliche und medizinische Informationen
- Rasse oder ethnische Herkunft
- Politische oder religiöse Überzeugungen
- Gewerkschaftsmitgliedschaften

3.3 Datenschutzgesetze

Viele Länder haben Datenschutzgesetze erlassen, die Anforderungen an die „Verarbeitung“ personenbezogener Daten festlegen. „Verarbeitung“ kann Maßnahmen wie Sammeln, Verwenden, Speichern, Ändern, Offenlegung, oder die Übermittlung personenbezogener Daten, unter anderem. So ist beispielsweise die Verarbeitung personenbezogener Daten von EU-Bürgern (einschließlich Kollegen und Antragstellern) so geregelt, dass jede Erhebung, Verarbeitung oder Übermittlung von Daten außerhalb der EU (oder anderer zugelassener Staaten) den Gesetzen wie den Allgemeinen Datenschutzvorschriften der EU (DSGVO) entsprechen muss.

Jede Übermittlung personenbezogener Daten aus der EU außerhalb der EU – wozu auch der Zugriff auf personenbezogene Daten aus der EU von außerhalb der EU gehört – erfordert vor der Datenübermittlung angemessene Garantien. Darüber hinaus erfordert die Weitergabe personenbezogener Daten aus der EU an Dritte (auch an Dritte, mit denen wir einen Vertrag geschlossen haben) außerhalb der EU angemessene Sicherheit und sollte mit der Rechtsabteilung und dem Leiter der Abteilung Ethik & Compliance koordiniert werden.

3.4 – Ihre Verantwortung für den Schutz von Mitarbeiterdaten

Kollegen und Auftragnehmer sind verpflichtet, alle für sie geltenden Aspekte dieser Richtlinie einzuhalten. Wenn Sie aufgrund Ihrer Rolle innerhalb des Unternehmens Zugriff auf personenbezogene Daten und/oder sensible personenbezogene Daten oder auf Daten anderer Personen haben, ist es Ihre Pflicht, von Energizer genehmigte Kontrollen einzuführen, um diese Daten zu sichern und zu schützen und den Zugriff auf die Daten nur auf diejenigen zu beschränken, die wissen müssen, und nur für notwendige und legitime Geschäftszwecke.

Energizer legt die folgenden Richtlinien für Kollegen fest, die auf Dateien mit personenbezogenen Daten oder sensiblen personenbezogenen Daten zugreifen, diese speichern und/oder übertragen (d. h. sie verarbeiten):

- i. Kennzeichnen Sie alle Dokumente, Dateien oder E-Mails, die sensible personenbezogene Daten enthalten, auffällig mit der folgenden Markierung:

„Persönlich und vertraulich“

- ii. Dateien, die diese Art von Daten enthalten, sollten nur an einem sicheren Speicherort wie OneDrive gespeichert werden, können aber **vorübergehend** auf gesicherten Unternehmensressourcen wie Laptops oder Desktop-Computern gespeichert werden und schließlich in OneDrive gespeichert werden.
- iii. Schützen Sie vertrauliche personenbezogene Daten mit Verschlüsselung und/oder Passwörtern. Vertrauliche personenbezogene Daten-Dateien sollten nur mit sicheren/verschlüsselten Methoden übertragen werden, wie z. B. Subject Line Encryption, Citrix ShareFile oder sicheren Übertragungsportalen mit einem Anbieter.
- iv. Bevor Sie personenbezogene EU-Daten und sensible personenbezogene Daten an Dritte weitergeben, stellen Sie sicher, dass diese sowohl angemessen als auch notwendig sind, und wenden Sie sich an die unten stehenden Datenschutzressourcen, um sicherzustellen, dass angemessene Schutzmaßnahmen getroffen werden.
- v. Denken Sie daran, Ihren Computer zu sperren, wenn Sie sich von ihm entfernen müssen.
- vi. Lassen Sie Ihren Laptop nicht in Sichtweite oder ungesichert in Ihrem Auto oder Hotelzimmer und gehen Sie nicht an öffentlichen Orten wie einem Flughafen davon weg.
- vii. Beachten Sie, dass selbst Daten wie Namen, E-Mail-Adressen und andere Informationen, die sich auf eine identifizierte oder identifizierbare Person beziehen, gemäß den Datenschutzgesetzen vieler Länder als „personenbezogene Daten“ angesehen werden können und zusätzliche Schutzmaßnahmen erfordern können.
- viii. Daten sollten von Ihrem Computer gelöscht werden, sobald Sie nicht mehr darauf zugreifen müssen, es sei denn, sie unterliegen einer Aufbewahrungsfrist für Rechtsstreitigkeiten oder einem anderen Zeitplan für die Aufbewahrung von Datensätzen.

Informieren Sie abschließend den Head of Ethics & Compliance, wenn Sie sich nicht sicher sind, ob bestimmte Informationen oder Dateien mit anderen Personen geteilt werden können, wenn Sie Kenntnis von vertraulichen Informationen erhalten, die versehentlich weitergegeben oder nicht autorisiert wurden, oder wenn Ihr Laptop oder Mobilgerät (Telefon oder Tablet) verloren gegangen, gestohlen oder kompromittiert wurde. Gestohlene Laptops oder mobile Geräte sollten ebenfalls dem IT Concierge gemeldet werden.

Section 4: Schutz vertraulicher oder proprietärer Unternehmensdaten

Vertrauliche Energizer-Daten

Vertrauliche Informationen sind Informationen, die Energizer, seine Kunden, Kollegen oder andere juristische oder natürliche Personen schädigen können, wenn sie unsachgemäß offengelegt werden, oder Informationen, die anderweitig nicht öffentlich zugänglich sind. Schäden können sich auf die Privatsphäre einer Person, die strategische Geschäftsposition von Energizer oder die seiner Kunden oder rechtliche oder behördliche Verpflichtungen beziehen. In Übereinstimmung mit Ihren Rollen und Verantwortlichkeiten haben Sie möglicherweise Zugriff auf vertrauliche Energizer-Daten.

Beispiele für vertrauliche Daten sind strategische Pläne, Marketingpläne, Finanzdaten, Kundenlisten, Verträge, Geschäftspläne, unveröffentlichte Patente, Geschäftsgeheimnisse, Fusionen und Übernahmen, Informationen, die einer Geheimhaltungsvereinbarung unterliegen, oder andere technische oder geschäftliche Informationen.

Diese Richtlinie erfordert den Schutz vertraulicher Daten bei der Speicherung, Verbreitung und Weitergabe innerhalb und außerhalb des Unternehmens unter Verwendung geeigneter administrativer, physischer und technischer Sicherheitsvorkehrungen, die den Risiken entsprechen, die durch den möglichen unbefugten Zugriff auf die Daten entstehen.

4.1 Ihre Verantwortung für den Schutz von Unternehmensdaten

Sofern sie nicht anders gekennzeichnet sind oder eindeutig als öffentliche Informationen bestimmt sind, behandeln Sie alle Informationen/Daten wie vertrauliche Energizer-Daten, unabhängig von ihrer Quelle oder Form, einschließlich elektronischer, gedruckter, mündlicher oder sonstiger Informationen.

Energizer legt die folgenden Richtlinien für den Zugriff auf, das Speichern und/oder die Übertragung (d. h. die Verarbeitung) von Dateien fest, die vertrauliche Energizer-Daten enthalten:

- Kennzeichnen Sie alle Dokumente, Dateien oder E-Mails, die vertrauliche Energizer-Daten enthalten, auffällig mit folgenden Punkten:

„Energizer proprietär und vertraulich“

- Dateien, die diese Art von Daten enthalten, sollten nur an einem sicheren Speicherort wie OneDrive gespeichert werden, können aber vorübergehend auf gesicherten Unternehmensressourcen wie Laptops oder Desktop-Computern gespeichert werden und schließlich in OneDrive gespeichert werden.
- Schützen Sie vertrauliche Daten mit entsprechenden Verschlüsselungen und/oder Kennwörtern und übertragen Sie sie nur mit sicheren Methoden, wie Subject Line Encryption, Citrix ShareFile oder sicheren Übertragungsportalen.

-
- Denken Sie daran, Ihren Computer zu sperren, wenn Sie sich von ihm entfernen müssen.
 - Lassen Sie Ihren Laptop nicht in Sichtweite oder ungesichert in Ihrem Auto oder Hotelzimmer und gehen Sie nicht an öffentlichen Orten wie einem Flughafen davon weg.
 - Vertrauliche Daten sollten von Ihrem Computer gelöscht werden, sobald Sie nicht mehr darauf zugreifen müssen, es sei denn, sie sind Gegenstand eines Rechtsstreits oder einer anderen, um den Energizer Aufbewahrungsplan für Aufzeichnungen einzuhalten.
 - Besprechen Sie vertrauliche Daten nur an nicht öffentlichen Orten oder indem Sie angemessene Maßnahmen ergreifen, um Gehör zu vermeiden.
 - Überprüfen, verteilen, kopieren und verteilen Sie vertrauliche Daten nur im erforderlichen Umfang und stellen Sie sicher, dass die empfangende Partei einer Geheimhaltungsvereinbarung oder ähnlichen Geheimhaltungsverpflichtungen unterliegt.

Geben Sie alle vertraulichen Daten zurück, die sich bei Beendigung Ihres Beschäftigungsverhältnisses in Ihrem Besitz befinden, und denken Sie daran, dass Ihre Verpflichtung zum Schutz vertraulicher Daten auch nach Beendigung des Beschäftigungsverhältnisses bestehen bleibt. **Wenn Sie feststellen, dass vertrauliche Daten (absichtlich oder unbeabsichtigt) an unbefugte Parteien weitergegeben wurden oder Ihr Laptop oder Mobilgerät verloren gegangen, gestohlen oder kompromittiert wurde und vertrauliche Daten enthielt, wenden Sie sich bitte umgehend an den Leiter für Ethics & Compliance und DEN IT-Concierge, um den Vorfall zu melden.**

Haben Sie eine Frage oder Bedenken?

Es gibt viele Möglichkeiten, eine Frage zu stellen oder Bedenken bezüglich dieser Politik zu äußern. Wählen Sie die Option, die Sie am bequemsten verwenden möchten. Welche Option Sie auch wählen, Ihre Vertraulichkeit wird respektiert, und Vergeltungsmaßnahmen werden nicht toleriert:

- Ihr Vorgesetzter oder die nächste Führungskraft
- Personalwesen
- Ethik und Compliance energizercompliance@energizer.com
- Legal
- Energizer-Hotline: www.EnergizerHelpLine.com
 - Rufen Sie unter der Nummer 1-877 521-5625 (USA) an.
 - Weitere Telefonnummern unter www.EnergizerHelpLine.com
 - Text „Bericht“ an 314-668-1383 (nur Nordamerika)
 - Sie können anonym bleiben, wenn Sie möchten
 - 24 Stunden verfügbar und von einem Drittanbieter betrieben

Section 5: Zugehörige Richtlinien und Standards

Policy-Name
Verhaltenskodex
Richtlinie Zur Annehmbaren Nutzung Der Informationstechnologie
Richtlinien für das Records and Information Management (RIM)

Section 6: Revisionshistorie

Der Policy-Verantwortliche überprüft und aktualisiert diese Policy bei Bedarf mindestens einmal pro Geschäftsjahr.

Revisionsnummer	Gültigkeitsdatum	Eigentümer	Beschreibung der Änderung
4	April 2024	Seth Smoker	Richtlinienverantwortlicher aktualisiert; „Head of Ethik & Compliance“ in „Associate General Counsel, Global Ethics & Compliance“ geändert und Kontaktinformationen in Karen Benson geändert
3	März 2021	Ronnie Kann	Aktualisierte Kontaktinformationen für Energizer-Helpline
2	November 2020	Ronnie Kann	Richtlinieneigentümer aktualisiert; „Chief Compliance Officer“ in „Head of Ethik & Compliance“ geändert; hinzugefügt, wie Fragen gestellt oder Bedenken geäußert werden können; Richtlinie und Verhaltenskodex VON RIM zu den entsprechenden Richtlinien und Standards hinzugefügt werden
1	Januar 2018	Kathy Rehmer	Neue Richtlinie

Section 7: Erforderliche Genehmigung

Signatur in Datei _____

Signatur in Datei _____



Policy globale sulla protezione dei dati

Data di entrata in vigore: Febbraio 2018

Ultima revisione: Aprile 2025

Section 1: Scopo della presente Informativa

La presente politica globale sulla protezione dei dati (la "politica") promuove un equilibrio efficace tra le pratiche di sicurezza delle informazioni e le esigenze aziendali, mantenendo al contempo la conformità alle leggi pertinenti. La politica aiuta Energizer a rispettare i nostri obblighi legali mantenendo la capacità dell'azienda di essere agile e soddisfare le aspettative dei clienti. Come illustrato più dettagliatamente di seguito, Energizer richiede diversi livelli di controlli di sicurezza a seconda della classificazione delle informazioni da proteggere, che si basano su rischi, praticità e altre considerazioni.

I nostri clienti, colleghi e altri si affidano a noi per proteggere le loro informazioni. Una violazione della sicurezza dei dati potrebbe danneggiare gravemente la nostra credibilità, causare perdite di affari e altri danni alle persone interessate. Una solida sicurezza dei dati richiede diligenza da parte di tutti i colleghi, appaltatori e di tutti gli altri che accedono o utilizzano le nostre risorse dati. La protezione dei dati fa parte del lavoro di tutti.

Principi guida

Tutti i colleghi devono tenere presenti i seguenti principi per la protezione dei dati:

- i. Energizer protegge la riservatezza, l'integrità e l'accesso alle proprie risorse di dati.
- ii. Energizer rispetterà le leggi applicabili sulla privacy e sulla protezione dei dati.
- iii. Energizer bilancia le esigenze di efficienza aziendale con l'esigenza di proteggere le informazioni personali, proprietarie e riservate da rischi inutili.
- iv. Energizer concede l'accesso a informazioni personali, proprietarie e di altro tipo riservate solo a coloro che hanno bisogno di conoscere e che sono obbligati a mantenere la sicurezza delle informazioni.
- v. I colleghi di Energizer sono la prima e migliore linea di difesa contro gli incidenti di sicurezza dei dati ed è responsabilità di ogni collega sostenere le pratiche di questa politica.
- vi. La rete, i sistemi e gli altri asset di Energizer sono principalmente a fini commerciali. Fatta eccezione per i casi in cui la legge applicabile prevede diversamente, l'utente non deve avere alcuna aspettativa di privacy quando utilizza la rete o i sistemi Energizer, incluse, a titolo esemplificativo ma non esaustivo, la trasmissione e l'archiviazione di file, dati e messaggi.

Section 2: Responsabile della politica e dichiarazione di responsabilità

La presente politica è di proprietà dell'associate General Counsel, Global Ethics & Compliance. E' responsabilità di questa persona, insieme all'ufficio legale, attuare, rivedere ogni anno e rivedere questa politica secondo necessità.



Policy globale sulla protezione dei dati

Data di entrata in vigore: Febbraio 2018

Ultima revisione: Aprile 2025

Nome	Titolo	Telefono	E-mail
Karen Benson	Associate General Counsel, Global Ethics & Compliance	954.593.6876	karen.benson@energizer.com

Section 3: Protezione dei dati personali

3.1 Raccolta ed elaborazione dei dati dei colleghi

Al fine di gestire in modo efficace la propria attività, Energizer deve raccogliere e utilizzare determinate informazioni personali sui colleghi. Le leggi e i regolamenti globali sulla privacy dei dati richiedono la raccolta, l'archiviazione, il trattamento, la condivisione, il trasferimento e l'uso appropriati dei dati personali, inclusi i dati personali dei colleghi ("dati personali dei colleghi"). È responsabilità fondamentale dei colleghi, come indicato nel codice di condotta, utilizzare i dati solo per lo scopo previsto e proteggerli in modo appropriato.

Alcuni dati, compresi dati personali sensibili e dati personali, sono raccolti da colleghi -- e in alcuni casi candidati -- da terzi autorizzati dall'azienda o dall'azienda a gestire tutti gli aspetti del lavoro, inclusi, a titolo esemplificativo ma non esaustivo: Stipendi, indennità, viaggi, rimborso spese, offerta online, amministrazione dei benefici, procedure disciplinari e di reclamo, tempi e presenze, gestione dei corsi di formazione e gestione delle carriere.

Se necessario per scopi aziendali e consentito dalla legge, Energizer può anche accedere e archiviare e-mail e documenti, inclusi CV, che possono contenere dati personali o sensibili. Energizer può anche raccogliere i dati dei colleghi quando monitora le comunicazioni e i sistemi per proteggere l'azienda da virus e malware o per garantire la conformità a policy, leggi e normative.

3.2 Tipi di dati dei colleghi raccolti

3.2(a) – Dati personali

Nell'Unione europea (UE) e in molti altri paesi, per "dati personali" si intendono in generale tutte le informazioni relative a una persona identificata o identificabile (ossia, una persona che può essere identificata direttamente o indirettamente facendo riferimento a un nome, un numero di identificazione, ecc.). In poche parole, i dati personali possono includere il nome di una persona, l'indirizzo e-mail, l'indirizzo fisico o simili.

3.2(b) – Dati personali sensibili

Le leggi sulla privacy dei dati variano a seconda del paese e alcuni elementi dei dati sono considerati sensibili in determinate giurisdizioni e richiedono una protezione aggiuntiva poiché l'uso inappropriato di questi dati può portare al furto di identità. Ad esempio, i dati personali sensibili possono includere:

- Informazioni sul conto bancario o sulla carta di credito (ad esempio numero di conto e numero di routing)
- Documento di identità nazionale, ad esempio numero di previdenza sociale
- Passaporto n.
- Informazioni sullo stipendio e sulla retribuzione correlata
- Informazioni biometriche, sanitarie e mediche
- Origine razziale o etnica
- Credenze politiche o religiose
- Membri sindacali

3.3 Leggi sulla protezione dei dati

Molti paesi hanno promulgato leggi sulla privacy dei dati che specificano i requisiti per il "trattamento" dei dati personali. Il "trattamento" può includere azioni quali la raccolta, l'utilizzo, la conservazione, la modifica, la divulgazione, o trasmettere dati personali, tra gli altri. Ad esempio, il trattamento dei dati personali dei cittadini dell'UE (compresi colleghi e richiedenti) è regolamentato in modo tale che qualsiasi raccolta, trattamento o trasferimento di dati al di fuori dell'UE (o di altri stati approvati) deve essere conforme alle leggi, come il regolamento generale sulla protezione dei dati (GDPR) dell'UE.

Qualsiasi trasferimento di dati personali dell'UE al di fuori dell'UE - che includa l'accesso ai dati personali dell'UE al di fuori dell'UE - richiede garanzie adeguate prima del trasferimento dei dati. Inoltre, la condivisione dei dati personali dell'UE con una terza parte (anche con quelle con cui abbiamo stipulato un contratto) al di fuori dell'UE richiede un'adeguata sicurezza e deve essere coordinata con l'ufficio legale e il responsabile dell'etica e della conformità.

3.4 – Le vostre responsabilità di proteggere i dati dei colleghi

I colleghi e gli appaltatori sono tenuti a rispettare tutti gli aspetti della presente politica che si applicano a loro. Se l'utente ha accesso ai dati personali e/o ai dati personali sensibili, o ai dati di altre persone in base al proprio ruolo all'interno della società, è suo dovere implementare controlli approvati da Energizer per proteggere e proteggere tali dati e limitare l'accesso ai dati solo a coloro che ne hanno bisogno e solo per scopi aziendali necessari e legittimi.

Energizer stabilisce le seguenti linee guida per i colleghi che accedono, salvano e/o trasmettono (ovvero elaborano) file con dati personali o dati personali sensibili:

- i. Contrassegnare chiaramente tutti i documenti, i file o le e-mail contenenti dati personali sensibili con il seguente contrassegno:

“Personale e riservato”

- ii. I file contenenti questo tipo di dati devono essere salvati solo in una posizione sicura come OneDrive, ma possono essere memorizzati **temporaneamente** su

Policy globale sulla protezione dei dati

Data di entrata in vigore: Febbraio 2018

Ultima revisione: Aprile 2025

-
- risorse aziendali protette, come computer portatili o desktop, eventualmente memorizzati in OneDrive.
- iii. Proteggete i file di dati personali sensibili con crittografia e/o password. I file di dati personali sensibili devono essere trasmessi solo utilizzando metodi sicuri/crittografati, come Subject Line Encryption, Citrix ShareFile o portali di trasmissione protetti con un fornitore.
 - iv. Prima di condividere i dati personali dell'UE e i dati personali sensibili con terzi, assicurarsi che siano appropriati e necessari e contattare le risorse sulla privacy riportate di seguito per garantire che siano predisposte adeguate misure di salvaguardia.
 - v. Ricordarsi di bloccare il computer se è necessario allontanarsi da esso.
 - vi. Non lasciare il computer portatile in bella vista, o non protetto, nella propria auto o in una camera d'albergo e non allontanarsi da esso in luoghi pubblici come un aeroporto.
 - vii. Tenere presente che anche dati quali nomi, indirizzi e-mail e altre informazioni relative a una persona identificata o identificabile possono essere considerati "dati personali" ai sensi delle leggi sulla privacy di molti paesi e potrebbero richiedere ulteriori protezioni.
 - viii. I dati devono essere eliminati dal computer non appena non è più necessario accedervi, a meno che non siano soggetti a conservazione a fini di contenzioso o ad altri piani di conservazione dei dati.

Infine, informare il responsabile dell'etica e della conformità se non si è sicuri che determinate informazioni o file possano essere condivisi con un'altra parte, se si viene a conoscenza di informazioni sensibili condivise per errore o non autorizzate, o se il laptop o il dispositivo mobile (telefono o tablet) è stato perso, rubato o compromesso. Anche i laptop o i dispositivi mobili rubati devono essere segnalati al concierge IT.

Section 4: Protezione dei dati riservati o proprietari dell'azienda

Dati riservati Energizer

Le informazioni riservate sono informazioni che possono danneggiare Energizer, i suoi clienti, colleghi o altre entità o individui se divulgate in modo improprio, o informazioni che non sono altrimenti disponibili al pubblico. I danni possono riguardare la privacy di un individuo, la posizione strategica commerciale di Energizer o quella dei suoi clienti, o le responsabilità legali o regolamentari. In base ai ruoli e alle responsabilità dell'utente, l'utente può avere accesso ai dati riservati di Energizer.

Esempi di dati riservati includono piani strategici, piani di marketing, dati finanziari, elenchi di clienti, contratti, piani aziendali, brevetti non pubblicati, segreti commerciali, documentazione M&A, informazioni soggette a un accordo di non divulgazione o altre informazioni tecniche o commerciali.

La presente politica richiede la protezione dei dati riservati nella conservazione, diffusione e condivisione sia all'interno che all'esterno dell'azienda, utilizzando adeguate garanzie

amministrative, fisiche e tecniche in base ai rischi posti dall'eventuale accesso non autorizzato ai dati.

4.1 Responsabilità dell'utente in materia di protezione dei dati aziendali

A meno che non siano contrassegnate diversamente o chiaramente destinate a essere informazioni pubbliche, trattare tutte le informazioni/dati come se fossero dati riservati di Energizer, indipendentemente dalla loro fonte o forma, incluse informazioni elettroniche, cartacee, verbali o di altro tipo.

Energizer stabilisce le seguenti linee guida per accedere, salvare e/o trasmettere (ovvero, elaborare) file contenenti dati riservati Energizer:

- Contrassegnare chiaramente tutti i documenti, i file o le e-mail che contengono dati riservati di Energizer con quanto segue:

"Energizer proprietario e riservato"

- I file contenenti questo tipo di dati devono essere salvati solo in una posizione sicura come OneDrive, ma possono essere memorizzati temporaneamente su risorse aziendali protette, come computer portatili o desktop, eventualmente memorizzati in OneDrive.
- Proteggere i dati riservati con la crittografia e/o le password appropriate e trasmettere solo utilizzando metodi sicuri, come Subject Line Encryption, Citrix ShareFile o portali di trasmissione sicuri.
- Ricordarsi di bloccare il computer se è necessario allontanarsi da esso.
- Non lasciare il computer portatile in bella vista, o non protetto, nella propria auto o in una camera d'albergo e non allontanarsi da esso in luoghi pubblici come un aeroporto.
- I dati riservati devono essere eliminati dal computer non appena non è più necessario accedervi, a meno che non siano soggetti a conservazione a fini di contenzioso o altro per rispettare il programma di conservazione dei dati di Energizer.
- Discutere i dati riservati solo in luoghi non pubblici o adottando misure ragionevoli per evitare di essere ascoltati.
- Eseguire la scansione, la distribuzione, la copia e la distribuzione dei dati riservati solo nella misura necessaria e assicurarsi che la parte ricevente sia soggetta a un accordo di non divulgazione o a obblighi analoghi di riservatezza.

Restituire tutti i dati riservati in suo possesso al termine del rapporto di lavoro e ricordare che l'obbligo di protezione dei dati riservati è scaduto anche dopo la cessazione del rapporto di lavoro. **Se si viene a conoscenza che i dati riservati sono stati condivisi con parti non autorizzate (intenzionalmente o involontariamente), oppure se il laptop o il dispositivo mobile è stato perso, rubato o compromesso e contengono**



Policy globale sulla protezione dei dati

Data di entrata in vigore: Febbraio 2018

Ultima revisione: Aprile 2025

dati riservati, contattare immediatamente il responsabile Etica e conformità e il concierge IT per segnalare l'incidente.

Hai una domanda o un problema?

Ci sono molti modi per porre una domanda o sollevare una preoccupazione in merito a questa politica. Scegliere l'opzione che si preferisce utilizzare. Qualunque opzione scegliate, la vostra riservatezza sarà rispettata e le ritorsioni non saranno tollerate:

- Il vostro manager o la leadership di livello successivo
- Risorse umane
- Etica e conformità energizercompliance@energizer.com
- Legale
- Numero di telefono Energizer: www.EnergizerHelpLine.com
 - Chiama il numero 1-877-521-5625 (Stati Uniti)
 - Ulteriori numeri di telefono all'indirizzo www.EnergizerHelpLine.com
 - Testo "Report" a 314-668-1383 (solo Nord America)
 - se lo si desidera, è possibile rimanere anonimi
 - disponibile 24 ore su 24 e gestito da un fornitore di terze parti

Section 5: Politiche e standard correlati

Nome criterio
Codice di condotta
Politica di utilizzo accettabile delle tecnologie informatiche
Politica RIM (record and Information Management)

Section 6: Cronologia revisioni

Il proprietario della politica esaminerà e aggiornerà questa politica secondo necessità almeno una volta ogni anno fiscale.

Numero di revisione	Data di entrata in vigore	Proprietario	Descrizione della modifica
4	Aprile 2024	Seth Smoker	"Il responsabile della politica è stato aggiornato; "responsabile dell'etica e della conformità" è stato modificato in "associate General Counsel, Global Ethics & Compliance" e le informazioni di contatto sono state modificate in Karen Benson.
3	Marzo 2021	Ronnie Kann	Informazioni di contatto aggiornate per la linea di assistenza Energizer



Policy globale sulla protezione dei dati

Data di entrata in vigore: Febbraio 2018

Ultima revisione: Aprile 2025

2	Novembre 2020	Ronnie Kann	Ha aggiornato il proprietario della policy; ha modificato il "Chief Compliance Officer" in "Head of Ethics & Compliance"; ha aggiunto come porre una domanda o segnalare un problema; ha aggiunto la politica RIM e il codice di condotta alle policy e agli standard correlati
1	Gennaio 2018	Kathy Rehmer	Nuova politica

Section 7: Approvazione richiesta

Firma su file _____

Firma su file _____

1 절: 정책의 목적

본 글로벌 데이터 보호 정책(이하 "정책")은 관련 법률을 준수하며 정보 보안 실무와 비즈니스 니즈 간의 균형을 효과적으로 증진합니다. 본 정책은 Energizer 가 민첩하게 비즈니스를 운영하고 고객의 기대를 만족시킴과 동시에 법적 의무를 이행하는 데 기여합니다. 하단에 자세히 명시되어 있듯이, Energizer 는 보호되어야 할 정보의 종류에 따라 상이한 보안 수준을 요구하며, 각 보안 수준은 위험성, 실용성 및 기타 고려 사항에 기반하여 결정됩니다.

고객, 직원, 기타 관계자는 당사가 그들의 정보를 보호해 줄 것으로 기대합니다. 데이터 보안이 침해될 경우, 회사에 대한 신뢰도가 저해되고 경제적 손실이 발생하며 관계자에게 피해를 줄 수 있습니다. 효과적인 데이터 보안 유지를 위해서는 전 직원, 계약업체 및 데이터 자산에 접근하거나 이를 이용하는 모든 사람들의 노력이 요구됩니다. 데이터 보호는 모든 직원의 의무입니다.

기본 원칙 모든 직원은 데이터 보호를 위해 다음의 원칙을

명심해야 합니다.

- i. Energizer 는 기밀 유지, 완결성 및 데이터 자산에 대한 접근성을 보장합니다. ii. Energizer 는 개인 정보 데이터 보호 및 데이터 보호 관련 법률을 준수할 것입니다.
- iii. Energizer 는 비즈니스 효율성에 대한 니즈와 개인 및 소유권 정보, 기타 기밀 정보를 불필요한 위험으로부터 보호해야 할 니즈 모두를 균형적으로 충족합니다. iv. Energizer 는 해당 정보를 알아야 하거나 이에 대한 보안을 유지할 의무를 지닌 사람에게는 개인 및 소유권 정보, 기타 기밀 정보에 접근할 수 있는 권리를 부여합니다.
- v. Energizer 직원은 데이터 보안 관련 사고를 방지하는 최초이자 최상의 위치에 있으며, 이러한 정책 방침을 준수하는 것은 모든 직원의 의무입니다.
- vi. Energizer 의 네트워크, 시스템 및 기타 자산은 비즈니스 운용을 주 목적으로 합니다. Energizer 의 파일, 데이터 및 메시지를 전송하고 저장하는 것과 더 나아가 네트워크 또는 시스템을 이용하는 경우에도 관련 법률에 다르게 규정된 경우를 제외하고, 예외 없이 본 정책을 준수해야 합니다.

2 절: 정책 소유자 및 책임 표시 사항

본 정책의 소유권은 개인 정보 데이터 책임자(Data Privacy Officer)에 귀속됩니다. 필요할 경우 법적 책임을 포함하여, 이 정책의 시행, 연례 검토 및 개정의 책임은 상기 개인에게 있습니다.

이름	직위	전화 번호	이메일
Karen Benson	준법무책임자, 글로벌 윤리 및 규정 준수	954.593.6876	karen.benson@energizer.com

3 절: 개인 데이터 보호

3.1 - 직원 데이터 수집 및 처리

Energizer 는 비즈니스의 효율적 운영을 위하여 직원들에 대한 일부 개인 정보를 수집 및 이용해야 합니다. 글로벌 개인 정보 데이터 보호 법규는 직원의 개인 데이터("직원 개인 데이터")를 포함하여 데이터의 수집, 저장, 처리, 공유, 전송하는 경우 및 기타 데이터 이용 시 적절한 방식을 적용할 것을 규정하고 있습니다. 윤리 강령에 명시된 것처럼 해당 목적 내에서만 데이터를 사용하고 이를 적절히 보호하는 행위는 직원으로서의 지켜야 할 기본 의무입니다.

중요 개인 데이터 및 기타 개인 데이터를 포함하여 직원(일부의 경우, 입사 지원자 포함)의 특정 데이터가 회사 또는 회사로부터 채용의 전반적인 측면을 관리하도록 위임받은 제 3 자에 의해 수집됩니다. 이러한 데이터에는 다음과 같은 사항이 포함되나 이에 한정되지는 않습니다. 급여, 보상, 여행, 비용, 상환, 온라인 지급, 수당 관리, 훈련 및 고충 처리 절차, 근무 시간 및 출결 정보, 훈련 과정 관리 및 경력 관리

비즈니스 목적을 위해 필요하고 법에 위반되지 않는 경우, Energizer 는 이력서를 포함하여 개인 정보나 중요 데이터가 담겨 있는 이메일 및 문서를 확인하고 이를 저장할 수도 있습니다. Energizer 는 회사가 바이러스나 악성 코드에 감염되는 것을 막거나 정책 및 법규를 준수하기 위하여 의사소통 및 시스템을 감시하는 과정에서 직원 데이터를 수집할 수도 있습니다.

3.2 수집되는 직원 데이터 유형

3.2(b) – 개인 데이터

유럽 연합(EU) 및 기타 많은 나라에서는, '개인 데이터'를 특정인 또는 식별이 가능한 개인과 관련된 모든 정보로 정의합니다(즉, 이름, ID 번호 등의 정보로 직접 또는 간접적으로 식별할 수 있는 사람). 간단히 말해, 개인 데이터에는 이름, 이메일 주소, 물리적 주소 및 이와 유사한 정보가 포함될 수 있습니다.

3.2(b) – 중요 개인 데이터

개인 정보 데이터 법률은 국가에 따라 상이하고, 일부 데이터 요소는 부적절하게 사용될 경우 신분 도용 문제를 야기할 수 있기 때문에 일부 사법 당국에서는 이를 민감한 것으로 간주하여 추가적인 보호 조치를 요구하기도 합니다. 예를 들어, 중요 개인 데이터에는 다음과 같은 사항이 포함될 수 있습니다.

- 계좌 정보 또는 신용 카드 정보(계좌 번호 및 은행 식별 기호)
- 사회 보장 번호 등 국가 신분증
- 여권 번호
- 급여 및 관련 수당 정보
- 생체인식 정보, 건강 및 의료 정보
- 인종 및 민족 출신 지역
- 정치적 또는 종교적 신념
- 노조 가입 여부

3.3 데이터 보호 법률

많은 국가들이 개인 데이터의 '처리'를 위한 구체적 요건을 정의하는 개인 정보 데이터 보호 법률을 제정했습니다. 우선, '처리'에는 개인 데이터의 수집, 사용, 저장, 변경, 공개 또는 전송 등의 행위가 포함됩니다. 예를 들어, EU 시민(직원 및 지원자 포함)의 개인 데이터 처리와 관련하여 모든 데이터 수집,

처리 또는 EU 외부(또는 기타 승인받은 국가)로의 전송은 EU 일반 개인 정보 보호법(GDPR)과 같은 법률을 반드시 준수해야 한다고 규정되어 있습니다.

EU 외부에서 EU 개인 정보를 전송(EU 외부에서의 EU 개인 데이터 접근 행위 포함)할 경우 사전에 적절한 안전 장치를 마련해야 합니다. 또한, EU 개인 데이터를 EU 외부의 제 3 자(Energizer 의 계약상대자도 포함)와 공유할 경우에도 적절한 안전 장치가 준비되어야 하며 법무 책임자 및 개인 정보 데이터 책임자의 협조를 얻어야 합니다.

3.4 - 직원 데이터 보호 의무

직원 및 계약업체는 자신에게 적용되는 본 정책의 모든 사항을 준수할 의무를 지닙니다. 회사 업무와 관련하여 개인 데이터 및/또는 중요 개인 데이터, 그 외 타인의 데이터에 접근할 경우, Energizer 로부터 승인을 받아 데이터를 관리함으로써 해당 데이터의 보안과 안전을 유지해야 하며, 해당 데이터를 알아야 하거나 적법한 비즈니스 목적을 수행하기 위해 필요한 사람에게만 이에 대한 접근을 제한적으로 허용해야 합니다.

Energizer 는 개인 데이터 또는 중요 개인 데이터를 포함한 파일을 이용, 저장 및/또는 전송(즉, 가공)하는 직원을 위한 가이드라인을 다음과 같이 제시합니다.

- i. 중요 개인 데이터를 포함한 모든 문서, 파일 또는 이메일에 다음과 같은 문구를 명확히 표시해야 합니다.

"개인 정보 및 기밀 사항"

- ii. 이러한 유형의 데이터를 포함한 파일은 원드라이브(OneDrive)와 같이 안전한 장소에만 보관하여야 하나, 노트북이나 데스크톱 컴퓨터와 같이 안전한 회사 자산에 **일시적으로** 저장할 수 있습니다. 그러나 이 경우에도 최종적으로는 해당 데이터를 원드라이브(OneDrive)로 옮겨 저장하여야 합니다.
- iii. 암호화 및/또는 비밀번호 설정을 통해 중요 개인 데이터 파일을 보호하십시오. 중요 개인 데이터 파일은 반드시 Subject Line Encryption, Citrix ShareFile 또는 공급업체와의 보안 전송 포털 등 안전한/암호화된 수단을 사용하여 전송되어야 합니다.

- iv. EU 개인 데이터 및 중요 개인 데이터를 제 3 자와 공유하기 전에, 반드시 해당 작업이 적절하고 필요한 행위인지 검토하고 하단의 개인 정보 보호 담당자에게 연락하여 적절한 안전 장치가 준비되었는지 확인해야 합니다.
- v. 자리를 비워야 할 때는 반드시 컴퓨터에 잠금 모드를 실행하십시오.
- vi. 노트북을 차량 내부나 호텔 방에 잘 보이게 두거나 안전하지 않은 상태로 두어서는 안 되며 공항과 같은 공공장소에 노트북만 두고 자리를 비워서는 안 됩니다.
- vii. 이름, 이메일 주소 및 기타 특징인 또는 식별 가능한 개인과 관련된 정보들도 많은 국가의 개인 정보 보호 법률에 의거하여 '개인 데이터'로 간주될 수 있으며 추가적인 보호 조치가 요구될 수 있다는 점에 유의하십시오.
- viii. 소송 대비용 또는 기타 기록물 보관 계획 관련 대상 데이터가 아닌 경우에는 데이터를 더 이상 이용할 필요가 없게 된 경우 즉시 이를 컴퓨터에서 삭제해야 합니다.

마지막으로, 특정 정보 또는 파일을 타인과 공유할 수 있는지 확인할 수 없는 경우, 무단으로 혹은 실수로 중요 정보를 공유했다는 사실을 인지한 경우, 또는 노트북이나 모바일 디바이스(휴대폰 또는 태블릿)를 분실, 도난당했거나 해당 기기에 문제가 발생한 경우에는 개인 정보 데이터 책임자 캐시 레머(Kathy.Rehmer@energizer.com), 또는 개인 정보 데이터 수석 변호사 앤디 화이트헤드(Andy.Whitehead@energizer.com)에게 연락하십시오. 노트북이나 모바일 디바이스를 도난당한 경우 IT Concierge 에게도 해당 사항을 보고해야 합니다.

4 절: 회사 기밀 및 소유권 데이터 보호

Energizer 기밀 데이터

기밀 데이터란 부적절하게 공개될 경우 Energizer 나 당사의 고객, 직원 또는 기타 조직 및 개인에게 피해를 줄 수 있는 정보 또는 대중에 공개되어서는 안 되는 정보를 의미합니다. 피해는 개인의 사생활, Energizer 이나 고객사의 전략적 비즈니스 포지션 또는 법규상의 의무와 관련될 수 있습니다. 귀하의 역할 및 의무에 따라, Energizer 기밀 데이터에 대한 접근이 허용될 수 있습니다.

기밀 데이터에는 전략 계획, 마케팅 계획, 재무 데이터, 고객 목록, 계약서, 비즈니스 플랜, 미발표 특허, 거래상 기밀, 인수 합병 문서, 기밀 유지 협약서의 적용을 받는 정보 또는 기타 기술이나 비즈니스 관련 정보가 포함됩니다.

본 정책에 따라 회사 내부 및 외부에서 저장, 배포 및 공유되는 기밀 데이터는 잠재적 무단 접근으로 인한 위험에 대비하기 위해 적절한 행정적, 물리적, 기술적 안전 장치를 통해 보호되어야 합니다.

4.1 회사 기밀 데이터 보호 의무

공개 대상 정보라고 표시되어 있거나 그러한 목적을 지닌 정보임이 분명한 경우를 제외하고는 모든 정보/데이터가 Energizer 의 기밀 데이터에 해당하는 것처럼 다루십시오. 이는 전자 문서, 종이 문서, 언어 또는 기타 정보 등 정보의 출처 또는 형태를 불문하고 적용됩니다.

Energizer 는 기밀 데이터를 포함한 파일을 이용, 저장 및/또는 전송(즉, 가공)하는 행위를 위한 가이드라인을 다음과 같이 제시합니다.

- 기밀 데이터를 포함한 모든 문서, 파일 또는 이메일에 다음과 같은 문구를 명확히 표시해야 합니다.

"Energizer 소유권 및 기밀 사항"

- 이러한 유형의 데이터를 포함한 파일은 원드라이브(OneDrive)와 같이 안전한 장소에만 보관하여야 하나, 노트북이나 데스크톱 컴퓨터와 같이 안전한 회사 자산에 **일시적으로** 저장할 수 있습니다. 그러나 이 경우에도 최종적으로는 해당 데이터를 원드라이브(OneDrive)로 옮겨 저장하여야 합니다.
- 암호화 및/또는 비밀번호 설정을 하고, Subject Line Encryption, Citrix ShareFile 또는 보안 전송 포털 등 안전한 수단을 통한 데이터 전송을 통해 기밀 데이터를 보호하십시오.
- 자리를 비워야 할 때는 반드시 컴퓨터에 잠금 모드를 실행하십시오.
- 노트북을 차량 내부나 호텔 방에 잘 보이게 두거나 안전하지 않은 상태로 두어서는 안 되며 공항과 같은 공공장소에 노트북만 두고 자리를 비워서는 안 됩니다.
- 소송 대비용 또는 기타 Energizer 의 기록물 보관(Records Retention) 계획 관련 대상 데이터가 아닌 경우에는 데이터를 더 이상 이용할 필요가 없게 된 경우 이를 즉시 컴퓨터에서 삭제해야 합니다.

- 기밀 데이터에 대해 논의할 경우에는 반드시 개방되지 않은 장소를 찾거나 타인에게 대화 내용이 들리지 않도록 적절한 조치를 취하십시오.
- 필요한 범위 내에서만 기밀 데이터를 스캔, 배포 또는 복사하고, 반드시 수신자가 기밀 유지 협약서 또는 이와 유사한 기밀 유지 의무를 준수하도록 하십시오.

퇴사하는 경우에는 보유하던 모든 기밀 데이터를 반납하여야 하며, 퇴사 이후에도 기밀 데이터 보호 의무가 존속된다는 것을 유념하십시오. 허가 받지 않은 타인에게 중요 정보를 공유(고의 또는 과실로)했다는 사실을 인지한 경우, 또는 기밀 데이터가 저장된 노트북이나 모바일 디바이스를 분실, 도난당했거나 해당 기기에 문제가 발생한 경우에는 즉시 개인 정보 데이터 책임자 및 IT 컨시어지에게 연락하여 문제 상황에 대해 보고하여 주십시오.

5 절: 관련 정책

정책 명칭
Information Technology Acceptable Use Policy(정보 기술 허용 사용자 정책)

6 절: 개정 이력 정책 소유자는 매 회계 연도 기준 1 회 이상 필요에 따라 이 정책을 검토하고 업데이트합니다.

개정 번호	발효일	소유자	변경 내역
4	2024 년 4 월	세스 흡연자	정책 담당자 업데이트, "윤리 및 규정 준수 책임자"를 "글로벌 윤리 및 규정 준수 담당 준법자문"으로 변경,

			연락처 정보를 Karen Benson 으로 변경
3	2021 년 3 월	로니 칸	Energizer 상담 전화의 연락처 정보가 업데이트되었습니다.
2	October 2022	Stephanie Ruttencutter	Replaced Kathy Rehmer with Ronnie Kann
버전 1	2018 년 1 월	캐시 레머(Kathy Rehmer)	신규 정책

7 절: 승인란

파일 확인 서명_____

파일 확인 서명_____

Część 1: cel niniejszych Zasad

Niniejsze Globalne zasady ochrony danych („Zasady”) promują skuteczną równowagę pomiędzy praktykami dotyczącymi bezpieczeństwa danych a potrzebami biznesowymi, przy jednoczesnym zachowaniu zgodności z odpowiednimi przepisami prawa. Zasady te pomagają firmie Energizer wywiązywać się ze zobowiązań prawnych przy zachowaniu zdolności do elastyczności i spełniania oczekiwań klientów. Zgodnie z przedstawionymi poniżej szczegółami firma Energizer wymaga różnych poziomów środków kontroli bezpieczeństwa, w zależności od stopnia tajności informacji, które mają być chronione, które oparte są na ryzyku, praktyczności i innych względach.

Klienci firmy Energizer, pracownicy i inne osoby polegają na firmie w zakresie ochrony ich informacji. Naruszenie bezpieczeństwa danych może poważnie zniszczyć wiarygodność firmy, narazić na straty gospodarcze i inne szkody osoby, których dotyczy ta sytuacja. Zdecydowane środki ochrony danych wymagają staranności ze strony wszystkich pracowników, kontrahentów i innych osób, które mają dostęp do zasobów danych i które ich używają. Ochrona danych należy do zakresu obowiązków każdej osoby.

Zasady przewodnie

Wszyscy współpracownicy powinni pamiętać o następujących zasadach ochrony danych:

- i. Firma Energizer ochroni poufność, integralność swoich zasobów danych, a także dostęp do nich.
- ii. Firma Energizer będzie przestrzegać obowiązujących przepisów prawa, które dotyczą prywatności i ochrony danych.
- iii. Firma Energizer równoważy potrzeby związane z efektywnością biznesową z potrzebą ochrony osobowych, zastrzeżonych i innych poufnych informacji przed niepotrzebnym ryzykiem.
- iv. Firma Energizer przyznaje dostęp do osobowych, zastrzeżonych i innych poufnych informacji jedynie tym osobom, które muszą je znać i które są zobowiązane do utrzymania bezpieczeństwa takich informacji.
- v. Pracownicy firmy Energizer są pierwszą i najlepszą linią obrony przed incydentami związanymi z bezpieczeństwem danych, a każdy pracownik ma obowiązek stosowania praktyk wynikających z niniejszych Zasad.
- vi. Sieć, systemy i inne zasoby firmy Energizer są przeznaczone głównie do celów biznesowych. Z wyjątkiem sytuacji, gdy obowiązujące prawo stanowi inaczej, Pracownik nie powinien oczekiwać prywatności podczas korzystania z sieci lub systemów firmy Energizer, w tym, między innymi, podczas przesyłania i przechowywania plików, danych i wiadomości.

Część 2: właściciel Zasad i oświadczenie o odpowiedzialności

Właścicielem niniejszych Zasad jest Dyrektor ds. ochrony danych. Osoba ta, wraz z działem prawnym, ma obowiązek każdego roku wdrażać, oceniać i sprawdzać niniejsze Zasady według potrzeb.

Imię i nazwisko	Stanowisko	Telefon	Adres e-mail
Karen Benson	Associate General Counsel, Global Ethics & Compliance	954.593.6876	karen.benson@energizer.com

Część 3: ochrona Danych osobowych

3.1 Gromadzenie i przetwarzanie Danych pracowników

Aby skutecznie prowadzić działalność, firma Energizer musi gromadzić i wykorzystywać określone dane osobowe swoich pracowników. Globalne przepisy ustawowe i wykonawcze w zakresie ochrony danych wymagają odpowiedniego gromadzenia, przechowywania, przetwarzania, udostępniania, przesyłania i używania danych osobowych, w tym danych osobowych pracowników („Danych osobowych pracowników”). Podstawowym obowiązkiem pracowników jest, jak wskazano w Kodeksie postępowania, używanie danych jedynie do celu, do którego były przeznaczone, a także stosowna ochrona tych danych.

Określone dane, w tym wrażliwe dane osobowe i dane osobowe, gromadzone są od pracowników — i w niektórych przypadkach kandydatów do pracy — przez firmę lub upoważnione przez firmę strony trzecie w celu zarządzania wszystkimi aspektami zatrudnienia, w tym, między innymi: listą płac, wynagrodzeniem, podróżami, zwrotem wydatków, dotacjami internetowymi, zarządzania świadczeniami, procedurami postępowania dyscyplinarnego i rozpatrywania skarg, terminowością i frekwencją, zarządzania szkoleniami i karierą.

Kiedy jest to konieczne do celów biznesowych i dopuszczalne przez prawo, firma Energizer może również uzyskać dostęp do wiadomości e-mail i dokumentów, w tym CV, które mogą zawierać dane osobowe lub wrażliwe, i może je przechowywać. Firma Energizer może również gromadzić dane pracowników, kiedy monitoruje komunikację i systemy w celu ochrony firmy przed wirusami i złośliwym oprogramowaniem oraz aby zapewnić zgodność z zasadami, przepisami ustawowymi i wykonawczymi.

3.2 Rodzaje gromadzonych Danych pracowników

3.2(a) — Dane osobowe

W Unii Europejskiej (UE) oraz w wielu innych krajach „dane osobowe” są ogólnie definiowane jako wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby (tj. osoby, którą można zidentyfikować bezpośrednio lub pośrednio przez odniesienie do imienia, numeru ewidencyjnego itp.). Krótko mówiąc, dane osobowe mogą zawierać imię i nazwisko osoby, adres e-mail, adres fizyczny lub podobne elementy.

3.2(b) — Wrażliwe dane osobowe

Przepisy prawa dotyczące ochrony danych różnią się w zależności od kraju. Niektóre elementy danych uważa się za wrażliwe w określonych jurysdykcjach i wymagają zastosowania dodatkowej ochrony, ponieważ niewłaściwe wykorzystanie tych danych może prowadzić do kradzieży tożsamości. Wrażliwe dane osobowe mogą obejmować na przykład:

- informacje dotyczące konta bankowego lub karty kredytowej (takie jak numer konta i numer rozliczeniowy);
- krajowy numer ewidencyjny, np. numer ubezpieczenia społecznego;
- numer paszportu;
- informacje dotyczące pensji i powiązanego wynagrodzenia;
- informacje biometryczne, medyczne i dotyczące zdrowia;
- pochodzenie rasowe lub etniczne; • przekonania polityczne lub religijne; • członkostwo w związkach.

3.3 Przepisy prawa dotyczące ochrony danych

W wielu krajach wprowadzone zostały przepisy prawa dotyczące ochrony danych, które określają wymogi związane z „przetwarzaniem” danych osobowych. „Przetwarzanie” może obejmować działania takie jak, między innymi, gromadzenie, używanie, przechowywanie, zmienianie, ujawnianie lub przysyłanie danych osobowych. Na przykład przetwarzanie danych osobowych obywateli UE (w tym pracowników i kandydatów do pracy) regulowane jest w taki sposób, że gromadzenie, przechowywanie lub przysyłanie danych poza teren UE (lub inne zatwierdzone kraje) musi być zgodne z przepisami prawa, np. z ogólnym rozporządzeniem Unii Europejskiej o ochronie danych (RODO).

Każde przysyłanie danych osobowych obywateli UE poza jej teren, które obejmuje uzyskanie dostępu do takich danych poza terenem UE, wymaga zastosowania odpowiednich zabezpieczeń przed przesłaniem danych. Dodatkowo udostępnianie danych osobowych obywateli UE stronie trzeciej (nawet takiej, z którą firma związana jest umową) poza teren UE wymaga zastosowania odpowiedniego zabezpieczenia i powinno być koordynowane przez dział prawny i Dyrektora ds. ochrony danych.

3.4 Odpowiedzialność Pracownika w zakresie ochrony danych pracowników

Pracownicy i kontrahenci są zobowiązani przestrzegać wszystkich aspektów niniejszych Zasad, które ich dotyczą. Jeżeli Pracownik ma dostęp do Danych osobowych i/lub Wrażliwych danych osobowych lub danych innej osoby na podstawie roli Pracownika w firmie, obowiązkiem Pracownika jest wdrożenie zatwierdzonych przez firmę Energizer środków kontroli w celu zabezpieczenia i ochrony takich danych, a także ograniczenia dostępu do danych jedynie do tych osób, które muszą znać dane i jedynie do niezbędnych i uzasadnionych celów biznesowych.

Firma Energizer określa następujące wytyczne dla pracowników, którzy mają dostęp do plików z Danymi osobowymi lub Wrażliwymi danymi osobowymi, zapisują je i/lub przesyłają (tj. przetwarzają):

- i. Należy w widoczny sposób oznaczyć wszystkie dokumenty, pliki lub wiadomości e-mail, które zawierają Wrażliwe dane osobowe, używając następującego oznaczenia:

„osobowe i poufne”

- ii. Pliki, które zawierają taki rodzaj danych, powinny być zapisywane jedynie w bezpiecznej lokalizacji, takiej jak OneDrive, ale mogą być **tymczasowo** przechowywane w zabezpieczonych zasobach firmy, takich jak laptop lub komputery stacjonarne, i ostatecznie przechowywane na dysku OneDrive.
- iii. Pliki z Wrażliwymi danymi osobowymi należy chronić za pomocą szyfrowania i/lub haseł. Pliki z Wrażliwymi danymi osobowymi powinny być przesyłane jedynie za pomocą bezpiecznych/zaszyfrowanych metod, takich jak szyfrowanie tematów wiadomości e-mail, rozwiązanie Citrix ShareFile lub portale dostawców do bezpiecznego przesyłania danych.
- iv. Przed udostępnieniem Danych osobowych i Wrażliwych danych osobowych obywateli UE stronom trzecim należy upewnić się, że działanie takie jest zarówno stosowne, jaki i konieczne, a także należy skontaktować się z wymienionymi poniżej osobami odpowiedzialnymi za ochronę danych, aby zapewnić, że zastosowane zostały odpowiednie zabezpieczenia.
- v. Należy pamiętać o zablokowaniu komputera, jeśli konieczne jest odejście od niego.
- vi. Nie należy zostawiać laptopa na widoku lub niezabezpieczonego, w samochodzie lub pokoju hotelowym i nie należy odchodzić od niego w miejscu publicznym, np. na lotnisku.
- vii. Należy pamiętać, że nawet dane takie jak imiona i nazwiska, adresy e-mail lub inne informacje, które dotyczą osoby zidentyfikowanej lub możliwej do zidentyfikowania mogą być uznawane za „Dane osobowe” według obowiązujących w wielu krajach przepisów prawa dotyczących ochrony danych i mogą wymagać zastosowania dodatkowych środków ochrony.
- viii. Dane powinny zostać usunięte z komputera Pracownika natychmiast po tym, gdy Pracownik nie potrzebuje już dostępu do nich, chyba że dane te podlegają prawnemu obowiązkowi przechowywania lub innemu harmonogramowi przechowywania dokumentacji.

Ostatecznie należy powiadomić Dyrektora ds. ochrony danych, Kathy Rehmer (Kathy.Rehmer@energizer.com), lub starszego doradcę ds. ochrony danych, Andy'ego Whiteheada (Andy.Whitehead@energizer.com), jeśli Pracownik nie ma pewności, czy określone informacje lub pliki mogą zostać udostępnione innej stronie, jeśli Pracownik dowie się o Danych wrażliwych, które zostały udostępnione przez pomyłkę lub bez upoważnienia lub jeśli laptop lub urządzenie przenośne (telefon bądź tablet) Pracownika został zgubiony, skradziony czy uszkodzony. Skradzione laptopy lub urządzenia przenośne powinny również zostać zgłoszone dyżurnemu konsultantowi IT.

Część 4: ochrona Danych poufnych lub Danych zastrzeżonych firmy

Dane poufne firmy Energizer

Dane poufne to informacje, które mogą zaszkodzić firmie Energizer, jej klientom, pracownikom lub innym podmiotom czy osobom, jeśli zostaną ujawnione w niewłaściwy sposób bądź są to informacje, które nie są podawane do wiadomości publicznej w inny sposób. Szkody mogą dotyczyć prywatności danej osoby, strategicznej pozycji biznesowej firmy Energizer lub jej klientów bądź zobowiązań prawnych czy regulacyjnych. Zgodnie ze swoją rolą i pełnionymi obowiązkami Pracownik może mieć dostęp do Danych poufnych firmy Energizer.

Przykładowe Dane poufne to: plany strategiczne, plany marketingowe, dane finansowe, listy klientów, umowy, plany biznesowe, nieopublikowane patenty, tajemnice handlowe, dokumentację dotyczącą fuzji i przejęć, informacje będące przedmiotem umowy o zachowaniu poufności lub inne informacje techniczne bądź biznesowe.

Niniejsze Zasady wymagają ochrony Danych poufnych w zakresie przechowywania, rozpowszechniania i udostępniania, zarówno wewnątrz firmy, jak i poza nią, za pomocą odpowiednich administracyjnych, fizycznych i technicznych zabezpieczeń zgodnie z ryzykiem związanym z ewentualnym uzyskaniem dostępu do danych przez osoby nieupoważnione.

4.1 Odpowiedzialność Pracownika w zakresie ochrony danych firmy

O ile nie zaznaczono inaczej lub o ile informacje nie są wyraźnie przeznaczone do stosowania jako Informacje publiczne, wszystkie informacje/dane należy traktować jako Dane poufne firmy Energizer, niezależnie od ich źródła lub formy, w tym informacje w formie elektronicznej, papierowej, ustnej lub inne.

Firma Energizer określa następujące wytyczne dotyczące uzyskiwania dostępu do plików zawierających Dane poufne firmy Energizer, ich zapisywania i/lub przesyłania (tj. przetwarzania):

- Należy w widoczny sposób oznaczyć wszystkie dokumenty, pliki lub wiadomości e-mail, które zawierają Dane poufne firmy Energizer, używając następującego oznaczenia:

„dokumenty zastrzeżone i poufne firmy Energizer”

- Pliki, które zawierają taki rodzaj danych, powinny być zapisywane jedynie w bezpiecznej lokalizacji, takiej jak OneDrive, ale mogą być **tymczasowo** przechowywane w zabezpieczonych zasobach firmy, takich jak laptop lub komputery stacjonarne, i ostatecznie przechowywane na dysku OneDrive.

- Należy chronić Dane poufne, stosując odpowiednie szyfrowanie i/lub hasła oraz przysyłać je, używając bezpiecznych metod, takich jak szyfrowanie tematów wiadomości e-mail, rozwiązanie Citrix ShareFile lub portale do bezpiecznego przesyłania plików.
 - Należy pamiętać o zablokowaniu komputera, jeśli konieczne jest odejście od niego.
 - Nie należy zostawiać laptopa na widoku lub niezabezpieczonego, w samochodzie lub pokoju hotelowym i nie należy odchodzić od niego w miejscu publicznym, np. na lotnisku.
 - Dane poufne powinny zostać usunięte z komputera Pracownika natychmiast po tym, kiedy Pracownik nie potrzebuje już dostępu do nich, chyba że dane te podlegają prawnemu obowiązowi przechowywania lub wymagane jest przestrzeganie obowiązującego w firmie Energizer harmonogramu przechowywania dokumentacji.
 - Dane poufne mogą być przedmiotem rozmów wyłącznie w miejscach innych niż publiczne lub po podjęciu uzasadnionych kroków, aby uniemożliwić ich podsłuchanie.
-
- Należy skanować, przekazywać i kopiować Dane poufne jedynie w niezbędnym zakresie. Należy również upewniać się, że strona otrzymująca podpisała umowę o zachowaniu poufności lub podlega innym podobnym zobowiązaniom do zachowania poufności.

Pracownik zobowiązany jest zwrócić wszystkie posiadane Dane poufne na koniec okresu zatrudnienia. Dodatkowo Pracownik jest zobowiązany do ochrony Danych poufnych, które będą istnieć po ustaniu zatrudnienia. **Jeśli Pracownik dowie się, że Dane poufne udostępniono nieupoważnionym stronom (umyślnie lub nieumyślnie) lub że laptop czy urządzenie przenośne Pracownika zostały zgubione, skradzione lub uszkodzone i zawierały Dane poufne, należy niezwłocznie skontaktować się Dyrektorem ds. ochrony danych i dyżurnym konsultantem IT w celu zgłoszenia incydentu.**

Część 5: powiązane Zasady

Nazwa Zasad
Zasady dopuszczalnego użytkowania technologii informatycznych

Część 6: historia zmian

Właściciel Zasad sprawdzi i zaktualizuje niniejsze Zasady w niezbędnym zakresie przynajmniej raz w każdym roku podatkowym.

Numer zmiany	Data wejścia w życie	Właściciel	Opis zmiany
4	Kwiecień 2024	Seth Smoker	Zaktualizowany właściciel polityki; zmienił „kierownik ds. etyki i zgodności” na „Associate General

			Counsel, Global Ethics & Compliance” i zmienił dane kontaktowe na Karen Benson
	Marzec 2021 r.	Ronnie Kann	Zaktualizowano informacje kontaktowe dla infolinii Energizer
Wersja 2	October 2022	Stephanie Ruttencutter	Updated Kathey Rehmer with Ronnie Kann
Wersja 1	styczeń 2018 r.	Kathy Rehmer	Nowe Zasady

Część 7: wymagana zgoda

Podpis
dokumentu

Podpis dokumentu

Seção 1: Finalidade desta Política

Esta Política Global de Proteção de Dados ("Política") promove um equilíbrio eficaz entre as práticas de segurança da informação e as necessidades comerciais, mantendo o cumprimento das leis relevantes. A Política ajuda a Energizer a cumprir nossas obrigações legais, mantendo a capacidade de agilidade do negócio e atender às expectativas dos clientes. Conforme descrito abaixo em mais detalhes, a Energizer requer diferentes níveis de controles de segurança, dependendo da classificação das informações a serem protegidas, que são baseadas em risco, praticidade e outras considerações.

Nossos clientes, colegas e outros confiam em nós para proteger suas informações. Uma violação de segurança de dados pode prejudicar gravemente a nossa credibilidade, causar perda de negócios e outros danos aos indivíduos afetados. A forte segurança dos dados requer diligência por parte de todos os colegas, contratantes e quaisquer outros que acessem ou utilizem os nossos ativos de dados. A proteção de dados faz parte do trabalho de todos.

Princípios orientadores

Todos os colegas devem ter em mente os seguintes princípios para a proteção de dados:

- i. A Energizer protege a confidencialidade, integridade e acesso aos seus ativos de dados.
- ii. A Energizer cumprirá as leis de privacidade e proteção de dados aplicáveis.
- iii. A Energizer equilibra as necessidades de eficiência empresarial com a necessidade de proteger informações pessoais, informações proprietárias e outras informações confidenciais contra riscos desnecessários.
- iv. A Energizer apenas concede acesso a informações pessoais, proprietárias e outras informações confidenciais àqueles com necessidade de saber e que são obrigados a manter a segurança das informações.
- v. Os colegas da Energizer são a primeira e melhor linha de defesa contra incidentes de segurança de dados, e é responsabilidade de todos os colegas manter as práticas desta Política.
- vi. A rede, sistemas e outros ativos da Energizer são principalmente para fins comerciais. Exceto quando a lei aplicável estabelecer o contrário, você não deve ter nenhuma expectativa de privacidade ao usar a rede ou sistemas da Energizer, incluindo, mas não limitado a, transmitir e armazenar arquivos, dados e mensagens.

Seção 2: Responsável pela Política e Declaração de Responsabilidade

Esta política é responsabilidade do Chefe do departamento de Ética e Compliance. É da responsabilidade deste indivíduo, juntamente com o Departamento Jurídico, implementar, rever anualmente e revisar esta política conforme necessário.

Nome	Responsável	Telefone	E-mail
Karen Benson	Consultor Geral Associado, Ética Global e Conformidade	954.593.6876	karen.benson@energizer.com

Seção 3: Proteção de Dados Pessoais

3.1 – Coleta e processamento de dados de colegas

Para gerir eficazmente o seu negócio, a Energizer precisa de coletar e utilizar determinadas informações pessoais sobre os nossos colegas. As leis e regulamentos globais de privacidade de dados exigem coleta, armazenamento, processamento, compartilhamento, transferência e uso apropriados de dados pessoais, incluindo os dados pessoais de colegas ("Dados Pessoais de Colega"). É de responsabilidade fundamental dos colegas, conforme descrito no Código de Conduta, utilizar os dados apenas para a finalidade que se pretendia e proteger adequadamente esses dados.

Certos dados, incluindo dados pessoais sensíveis e dados pessoais, são coletados de colegas - e, em alguns casos, candidatos a emprego - seja pela empresa ou por terceiros autorizados pela empresa para administrar todos os aspetos da relação empregatícia, incluindo, mas não se limitando a: Folha de pagamento, compensação, viagem, reembolso de despesas, doação on-line, administração de benefícios, procedimentos disciplinares e de queixas, tempo e frequência, gestão de cursos de formação e gestão de carreira.

Quando necessário para fins comerciais, e permitido por lei, a Energizer também pode acessar e armazenar e-mails e documentos, incluindo currículos (CVs), que podem conter dados pessoais ou confidenciais. A Energizer também pode coletar dados de colegas quando monitora comunicações e sistemas para proteger a empresa contra vírus e malware ou para garantir a conformidade com políticas, leis e regulamentos.

3.2 Tipos de Dados Pessoais de Colegas Coletados

3.2(a) – Dados Pessoais

Na União Europeia (UE) e em muitos outros países, os "dados pessoais" são amplamente definidos como qualquer informação relativa a uma pessoa identificada ou identificável (isto é, uma pessoa que pode ser identificada direta ou indiretamente por referência a um nome, número de identificação, etc.). Simplificando, os dados pessoais podem incluir o nome de uma pessoa, endereço de e-mail, endereço físico ou similares.

3.2(b) – Dados Pessoais Sensíveis

As leis de privacidade de dados variam de acordo com o país e alguns elementos de dados são considerados sensíveis em determinadas jurisdições e exigem proteção adicional, pois o uso inadequado desses dados pode levar ao roubo de identidade. Por exemplo, os dados pessoais sensíveis podem incluir:

- Informações de conta bancária ou cartão de crédito (como número de conta))

-
- Identificação nacional, como número de Segurança Social
 - Número do Passaporte
 - Informações sobre remuneração e informações relacionadas
 - Informações biométricas, de saúde e médicas
 - Origem racial ou étnica
 - Crenças políticas ou religiosas
 - Associações sindicais

3.3 – Leis de proteção de dados

Muitos países promulgaram leis de privacidade de dados que especificam requisitos para o "processamento" de dados pessoais. "Processamento" pode incluir ações como coletar, usar, armazenar, alterar, divulgar, ou transmitir dados pessoais, entre outros. Por exemplo, o processamento de dados pessoais de cidadãos da União Europeia (UE) (incluindo colegas e candidatos) é regulado de forma a que qualquer recolha, tratamento ou transferência de dados para fora da UE (ou outros estados aprovados) deve cumprir as leis, como o Regulamento Geral de Proteção de Dados da UE (RGPD).

Qualquer transferência de dados pessoais da UE para fora da UE - que inclui o acesso aos dados pessoais da UE de fora da UE - requer salvaguardas adequadas antes da transferência de dados. Além disso, o compartilhamento de dados pessoais da UE com terceiros (mesmo aqueles com quem temos um contrato) fora da UE requer segurança adequada e deve ser coordenado com o Departamento Jurídico e com o Chefe do Departamento de Ética e Compliance.

3.4 – Suas responsabilidades para proteger os dados do colega

Colegas e contratados são obrigados a cumprir todos os aspetos desta Política que se aplicam a eles. Se você tiver acesso a Dados Pessoais e/ou Dados Pessoais Sensíveis, ou a dados de outros indivíduos com base em sua função dentro da Empresa, é seu dever implementar controles aprovados pela Energizer para proteger esses dados e limitar o acesso aos dados apenas àqueles que precisame apenas para fins comerciais necessários e legítimos.

A Energizer estabelece as seguintes diretrizes para colegas que estão acessando, salvando e/ou transmitindo (ou seja, processando) arquivos com Dados Pessoais ou Dados Pessoais Sensíveis:

- i. Marque de forma visível todos os documentos, arquivos ou e-mails que contenham Dados Pessoais Sensíveis com a seguinte marcação:

"Pessoal e Confidencial"

- ii. Os arquivos que contêm esse tipo de dados devem ser salvos apenas em um local seguro, como o OneDrive, mas podem ser **armazenados temporariamente** em recursos protegidos da empresa, como laptops ou computadores desktop, e eventualmente armazenados no OneDrive.
- iii. Proteja arquivos de dados pessoais confidenciais com criptografia e/ou senhas. Os arquivos de

dados pessoais confidenciais só devem ser transmitidos usando métodos seguros/criptografados, como Criptografia de linha de assunto, Citrix ShareFile ou portais de transmissão seguros com um fornecedor.

- iv. Antes de compartilhar Dados Pessoais e Dados Pessoais Sensíveis com terceiros, certifique-se de que são adequados e necessários e contate os Recursos de Privacidade abaixo para garantir a existência de salvaguardas adequadas.
- v. Lembre-se de bloquear o computador se você precisar se afastar dele.
- vi. Não deixe o seu computador portátil à vista, ou em local não seguro, no seu carro ou num quarto de hotel e não se afaste dele num local público, como um aeroporto.
- vii. Esteja ciente de que mesmo dados como nomes, endereços de e-mail e outras informações relacionadas a uma pessoa identificada ou identificável podem ser considerados "Dados Pessoais" sob as leis de privacidade de muitos países e podem exigir proteções adicionais.
- viii. Os dados devem ser excluídos do seu computador assim que você não tiver mais necessidade de acessá-los, a menos que esteja sujeito a contencioso ou outro cronograma de retenção de registros.

Por fim, notifique o Chefe do departamento de Ética e Compliance se não tiver certeza se determinadas informações ou ficheiros podem ser compartilhados com outra parte, se tiver conhecimento de informações sensíveis que foram compartilhadas por engano ou não autorizadas, ou se o seu computador portátil ou dispositivo móvel (telefone ou tablet) foi perdido, roubado ou comprometido. Laptops roubados ou dispositivos móveis também devem ser comunicados ao responsável por Tecnologia da Informação (TI).

Seção 4: Protegendo os Dados Confidenciais ou de propriedade da Empresa

Informações Confidenciais são informações que podem causar danos à Energizer, seus clientes, colegas ou outras entidades ou indivíduos se forem divulgadas indevidamente, ou informações que não estejam disponíveis publicamente de outra forma. Os danos podem estar relacionados com a privacidade de um indivíduo, a posição estratégica de negócios da Energizer ou de seus clientes, ou com responsabilidades legais ou regulatórias. De acordo com suas funções e responsabilidades, você pode ter acesso aos Dados Confidenciais da Energizer.

Exemplos de Dados Confidenciais incluem planos estratégicos, planos de marketing, dados financeiros, listas de clientes, contratos, planos de negócios, patentes não publicadas, segredos comerciais, documentação de M&A, informações sujeitas a um acordo de não divulgação ou outras informações técnicas ou comerciais.

Esta Política requer a proteção de Dados Confidenciais no armazenamento, divulgação e compartilhamento dentro e fora da empresa, usando salvaguardas administrativas, físicas e técnicas apropriadas de acordo com os riscos decorrentes do possível acesso não autorizado aos dados.

4.1 Suas responsabilidades para proteger os dados da empresa

A menos que esteja marcado de outra forma ou claramente destinado a ser Informação Pública, trate todas as informações/dados como se fossem Dados Confidenciais da Energizer, independentemente de sua fonte ou forma, incluindo informações eletrônicas, em papel, verbais ou outras.



Política Global de Proteção de Dados

Data de vigência: Fevereiro de 2018

A Energizer estabelece as seguintes diretrizes para acessar, salvar e/ou transmitir (ou seja, processar) arquivos que contenham Dados Confidenciais da Energizer:

- Marque de forma visível todos os documentos, arquivos ou e-mails que contenham Dados Confidenciais da Energizer com o seguinte:

"Propriedade da Energizer e Confidencial" "

- Os arquivos que contêm esse tipo de dados devem ser salvos apenas em um local seguro, como o OneDrive, mas podem ser **armazenados temporariamente** em recursos protegidos da empresa, como laptops ou computadores desktop, eventualmente armazenados no OneDrive.
- Proteja os dados confidenciais com criptografia e/ou senhas apropriadas e transmita somente usando métodos seguros, como Criptografia de linha de assunto, Citrix ShareFile ou portais de transmissão seguros.
- Lembre-se de bloquear o computador se você precisar se afastar dele.
- Não deixe o seu computador portátil à vista, ou em local não seguro, no seu carro ou num quarto de hotel e não se afaste dele num local público, como um aeroporto.
- Os Dados Confidenciais devem ser excluídos do seu computador assim que você não tiver mais necessidade de acessá-los, a menos que esteja sujeito a contencioso ou outro para cumprir o cronograma de Retenção de Registros da Energizer.
- Discuta apenas os Dados Confidenciais em locais não públicos ou tomando medidas razoáveis para evitar que sejam ouvidos.
- Apenas digitalize, distribua copie e compartilhe Dados Confidenciais na medida do necessário e garanta que a parte recebedora esteja sujeita a um acordo de não divulgação ou sob obrigações semelhantes de confidencialidade.

Devolva todos os Dados Confidenciais em sua posse no final do seu contrato de trabalho e lembre-se de que sua obrigação de proteger dados confidenciais permanece após o término do emprego. **Se tomar conhecimento de que os Dados Confidenciais foram compartilhados com terceiros não autorizados (intencionalmente ou não), ou se o seu computador portátil ou dispositivo móvel foi perdido, roubado ou comprometido e continha Dados Confidenciais, contate imediatamente o Chefe do departamento de Ética e Compliance e o responsável por TI para comunicar o incidente.**

Tem uma pergunta ou uma preocupação?

Há muitas maneiras de fazer uma pergunta ou levantar uma preocupação em relação a esta política. Escolha a opção que você está mais confortável usando. Seja qual for a opção escolhida, a sua confidencialidade será respeitada e a retaliação não será tolerada:

- Seu gerente ou liderança de nível seguinte
- Recursos Humanos
- Departamento de Ética e Compliance em energizercompliance@energizer.com
- Departamento Jurídico
- Canal de denúncias da Energizer: www.EnergizerHelpLine.com,

o Ligue 1-877-521-5625 (EUA)



Política Global de Proteção de Dados

Data de vigência: Fevereiro de 2018

- Números de telefone adicionais em www.EnergizerHelpLine.com
 - Envie "Relatório" para 314-668-1383 (apenas América do Norte)
 - você pode permanecer anônimo se você escolher
 - disponível 24 horas e operado por um provedor terceirizado

Seção 5: Políticas e padrões relacionados

Nome da política
Código de Conduta Política de Registros de Política de Uso Aceitável e Gerenciamento de Informações (RIM) de Tecnologia da Informação

Seção 6: Histórico de revisões

O responsável pela política analisará e atualizará esta política conforme necessário, pelo menos uma vez a cada ano fiscal.

Revisão Número	Data Efetiva	Responsável	Descrição da mudança
4	Abril de 2024	Seth Smoker	Proprietário da política atualizado; mudou "chefe de ética e conformidade" para "Conselheiro geral associado, Ética global e conformidade" e mudou as informações de contato para Karen Benson
3	Março de 2021	Ronnie Kann	Informações de contacto atualizadas para a linha de assistência da Energizer
2	Novembro de 2020	Ronnie Kann	Responsável da política atualizado; mudou "conformidade principal Diretor" para "chefe de ética e conformidade"; acrescentou como fazer uma pergunta ou levantar uma preocupação; adicionou a política e o código de conduta da RIM às políticas e padrões relacionados
1	Janeiro de 2018	Kathy Rehmer	Nova política

Seção 7: Aprovação necessária

Assinatura em arquivo _____

Assinatura em arquivo _____



Глобальная политика защиты данных

Дата вступления в силу: Февраль 2018 года

Последняя редакция: Апрель 2025 года

Section 1: Цель настоящей политики

Настоящая Глобальная политика защиты данных («Политика») способствует эффективному балансу между практиками информационной безопасности и потребностями бизнеса, сохраняя при этом соблюдение соответствующих законов. Политика помогает Energizer выполнять наши юридические обязательства, сохраняя при этом способность бизнеса быть гибким и соответствовать ожиданиям клиентов. Как более подробно описано ниже, Energizer требует различных уровней контроля безопасности в зависимости от классификации защищаемой информации, которые основаны на риске, практичности и других соображениях.

Наши клиенты, коллеги и другие люди полагаются на нас для защиты их информации. Нарушение безопасности данных может серьезно подорвать доверие к нам, привести к потере бизнеса и другому ущербу пострадавшим лицам. Надежная защита данных требует тщательной проверки со стороны всех коллег, подрядчиков и любых других лиц, получающих доступ к нашим информационным ресурсам или использующих их. Защита данных является частью работы каждого.

Руководящих принципов

Все коллеги должны помнить о следующих принципах защиты данных:

- i. Energizer защищает конфиденциальность, целостность и доступ к своим информационным активам.
- ii. Компания Energizer будет соблюдать применимые законы о конфиденциальности и защите данных.
- iii. Energizer сочетает потребности в эффективности бизнеса с необходимостью защиты личной, служебной и другой конфиденциальной информации от ненужного риска.
- iv. Energizer предоставляет доступ только к личной, служебной и другой конфиденциальной информации тем, кто должен знать и кто обязан поддерживать безопасность информации.
- v. Коллеги Energizer являются первой и лучшей линией защиты от инцидентов, связанных с безопасностью данных, и каждый коллега несет ответственность за соблюдение практики настоящей политики.
- vi. Сеть, системы и другие активы Energizer предназначены в первую очередь для бизнес-целей. За исключением случаев, когда применимое законодательство предусматривает иное, вы не должны ожидать конфиденциальности при использовании сети или систем Energizer, включая, но не ограничиваясь, передачу и хранение файлов, данных и сообщений.

Section 2: Владелец политики и заявление об ответственности

Данная политика принадлежит заместителю Генерального юрисконсульта по вопросам глобальной этики и комплаенса. Это лицо, наряду с юридическим, несет ответственность



Глобальная политика защиты данных

Дата вступления в силу: Февраль 2018 года

Последняя редакция: Апрель 2025 года

за осуществление, пересмотр ежегодно и пересмотр этой политики по мере необходимости.

Имя	Заголовок	Телефон	Электронная почта
Karen Benson	Заместитель главного юрисконсульта по вопросам глобальной этики и комплаенса	954.593.6876	karen.benson@energizer.com

Section 3: Защита персональных данных

3.1 Сбор и обработка данных коллег

Для эффективного ведения бизнеса Energizer необходимо собирать и использовать определенную личную информацию о наших коллегах. Глобальные законы и нормативные акты о конфиденциальности данных требуют надлежащего сбора, хранения, обработки, совместного использования, передачи и использования персональных данных, включая персональные данные коллег («Персональные данные коллег»). Как указано в Кодексе поведения, основная ответственность за использование данных только в тех целях, в которых они были задуманы, и надлежащую защиту этих данных лежит на коллегах.

Определенные данные, включая конфиденциальные персональные данные и персональные данные, собираются от коллег - и в некоторых случаях кандидатов на работу - либо компанией или уполномоченными третьими лицами компании для управления всеми аспектами занятости, включая, но не ограничиваясь: Заработную плату, компенсацию, поездки, возмещение расходов, онлайн-предоставление, администрирование пособий, дисциплинарные процедуры и процедуры рассмотрения жалоб, время и посещаемость, управление учебными курсами и управление карьерой.

Когда это необходимо для деловых целей и разрешено законом, Energizer может также получать доступ и хранить электронные письма и документы, включая резюме (CV), которые могут содержать личные или конфиденциальные данные. Компания Energizer также может собирать данные коллег при мониторинге коммуникаций и систем для защиты бизнеса от вирусов и вредоносных программ или для обеспечения соответствия политикам, законам и нормативным актам.

3.2 Типы собранных данных коллег

3.2(a) — Персональные данные

В Европейском союзе (ЕС) и многих других странах «персональные данные» широко определяются как любая информация, относящаяся к идентифицируемому или идентифицируемому лицу (т.е. лицу, которое может быть идентифицировано прямо или косвенно посредством ссылки на имя, идентификационный номер и т.д.). Проще говоря,

личные данные могут включать имя человека, адрес электронной почты, физический адрес или тому подобное.

3.2(b) Конфиденциальные персональные данные

Законы о конфиденциальности данных различаются в зависимости от страны, и некоторые элементы данных считаются чувствительными в определенных юрисдикциях и требуют дополнительной защиты, поскольку ненадлежащее использование этих данных может привести к краже личных данных. Например, конфиденциальные персональные данные могут включать:

- Информация о банковском счете или кредитной карте (например, номер счета и номер маршрута)
- Национальный идентификатор, например номер социального страхования
- Паспорт #
- Информация о заработной плате и связанных с ней компенсациях
- Биометрическая, медицинская и медицинская информация
- Расового или этнического происхождения
- Политических или религиозных убеждений
- Членство в союзе

3.3 Законы о защите данных

Многие страны приняли законы о конфиденциальности данных, которые определяют требования для «обработки» персональных данных. «Обработка» может включать такие действия, как сбор, использование, хранение, изменение, раскрытие, или передачи персональных данных, среди прочего. Например, обработка персональных данных граждан ЕС (включая коллег и заявителей) регулируется таким образом, что любой сбор, обработка или передача данных за пределы ЕС (или других утвержденных государств) должен соответствовать законам, таким как Общие правила защиты данных ЕС (GDPR).

Любая передача персональных данных ЕС за пределы ЕС, которая включает в себя доступ к персональным данным ЕС из-за пределов ЕС, требует соответствующих гарантий перед передачей данных. Кроме того, передача персональных данных ЕС третьей стороне (даже тем, с кем у нас есть контракт) за пределами ЕС требует надлежащей безопасности и должна координироваться с юридическим отделом и руководителем отдела этики и комплаенса.

3.4 Ваши обязанности по защите данных коллег

Коллеги и подрядчики обязаны соблюдать все аспекты настоящей политики, которые относятся к ним. Если у вас есть доступ к персональным данным и/или конфиденциальным персональным данным или данным другого лица на основе вашей роли в компании, вы обязаны внедрить одобренные Energizer средства контроля для защиты и защиты этих



Глобальная политика защиты данных

Дата вступления в силу: Февраль 2018 года

Последняя редакция: Апрель 2025 года

данных и ограничить доступ к данным только теми, кому необходимо знать, и только для необходимых и законных деловых целей.

Energizer устанавливает следующие рекомендации для коллег, которые получают доступ, сохраняют и/или передают (т.е. обрабатывают) файлы с персональными данными или конфиденциальными персональными данными:

- i. Отметьте все документы, файлы или электронные письма, содержащие конфиденциальные персональные данные, следующей маркировкой:

«Личные и конфиденциальные»

- ii. Файлы, содержащие данные такого типа, должны сохраняться только в безопасном месте, например OneDrive, но могут **временно** храниться на защищенных ресурсах компании, таких как ноутбуки или настольные компьютеры, в конечном итоге храниться в OneDrive.
- iii. Защита конфиденциальных файлов персональных данных с помощью шифрования и/или паролей. Конфиденциальные файлы персональных данных должны передаваться только с использованием защищенных/зашифрованных методов, таких как шифрование строки темы, Citrix ShareFile или безопасные порталы передачи с поставщиком.
- iv. Прежде чем делиться персональными данными ЕС и конфиденциальными персональными данными с третьими лицами, убедитесь, что это уместно и необходимо, и обратитесь к ресурсам конфиденциальности ниже, чтобы обеспечить надлежащие меры предосторожности.
- v. Не забудьте заблокировать компьютер, если вам нужно отойти от него.
- vi. Не оставляйте ноутбук на виду или без безопасности в автомобиле или номере отеля и не отходите от него в общественном месте, например в аэропорту.
- vii. Имейте в виду, что даже такие данные, как имена, адреса электронной почты и другая информация, которая относится к идентифицированному или идентифицируемому лицу, могут считаться «персональными данными» в соответствии с законами о конфиденциальности многих стран и могут потребовать дополнительной защиты.
- viii. Данные должны быть удалены с вашего компьютера, как только у вас больше нет необходимости в доступе к ним, за исключением случаев, когда на них распространяются судебные разбирательства или другие сроки хранения записей.

И наконец, сообщите об этом руководителю отдела этики и комплаенса, если вы не уверены, можно ли поделиться определенной информацией или файлами с другой стороной, если вам стало известно о конфиденциальной информации, которая была передана по ошибке или несанкционированно, или если ваш ноутбук или мобильное устройство (телефон или планшет) были утеряны, украдены или



Глобальная политика защиты данных

Дата вступления в силу: Февраль 2018 года

Последняя редакция: Апрель 2025 года

скомпрометированы. Об украденных ноутбуках или мобильных устройствах также следует сообщить ИТ-консьержу.

Section 4: Защита конфиденциальных или служебных данных компании

Конфиденциальные данные Energizer

Конфиденциальная информация — это информация, которая может причинить вред компании Energizer, ее клиентам, коллегам или другим организациям или физическим лицам, если она раскрыта ненадлежащим образом, или информация, которая иным образом не является общедоступной. Вред может быть связан с конфиденциальностью лица, стратегической деловой позицией Energizer или ее клиентов, а также с юридическими или нормативными обязательствами. В соответствии с вашими ролями и обязанностями вы можете иметь доступ к конфиденциальным данным Energizer.

Примеры конфиденциальных данных включают стратегические планы, маркетинговые планы, финансовые данные, списки клиентов, контракты, бизнес-планы, неопубликованные патенты, коммерческая тайна, документация по слияниям и Поглощениям, информация, подпадающая под действие соглашения о неразглашении, или другая техническая или деловая информация.

Настоящая Политика требует защиты конфиденциальных данных при хранении, распространении и совместном использовании как внутри компании, так и за ее пределами с использованием соответствующих административных, физических и технических средств защиты в соответствии с рисками, связанными с возможным несанкционированным доступом к данным.

4.1 Ваши обязанности по защите данных компании

Если она не помечена иным образом или явно предназначена для публичной информации, обращайтесь со всей информацией/данными так, как если бы это были Конфиденциальные данные Energizer, независимо от ее источника или формы, включая электронную, бумажную, устную или другую информацию.

Energizer устанавливает следующие рекомендации по доступу, сохранению и/или передаче (т.е. обработке) файлов, содержащих конфиденциальные данные Energizer:

- Отметьте все документы, файлы или сообщения электронной почты, содержащие конфиденциальные данные Energizer, следующим образом:



Глобальная политика защиты данных

Дата вступления в силу: Февраль 2018 года

Последняя редакция: Апрель 2025 года

«Energizer является собственностью и конфиденциальностью»

- Файлы, содержащие данные такого типа, должны сохраняться только в безопасном месте, например OneDrive, но могут временно храниться на защищенных ресурсах компании, таких как ноутбуки или настольные компьютеры, в конечном итоге храниться в OneDrive.
- Защитите конфиденциальные данные с помощью соответствующего шифрования и/или паролей и передавайте их только с помощью безопасных методов, таких как шифрование строки темы, Citrix ShareFile или безопасные порталы передачи.
- Не забудьте заблокировать компьютер, если вам нужно отойти от него.
- Не оставляйте ноутбук на виду или без безопасности в автомобиле или номере отеля и не отходите от него в общественном месте, например в аэропорту.
- Конфиденциальные данные должны быть удалены с вашего компьютера, как только у вас больше нет необходимости в доступе к ним, если только они не подлежат судебному задержанию или иным образом в соответствии с графиком хранения записей Energizer.
- Обсуждайте конфиденциальные данные только в непубличных местах или предпринимайте разумные меры, чтобы не быть услышанным.
- Сканируйте, распространяйте, копируйте и распространяйте Конфиденциальные данные только в той мере, в какой это необходимо, и убедитесь, что получающая сторона подпадает под действие соглашения о неразглашении или аналогичных обязательств по конфиденциальности.

Верните все конфиденциальные данные, находящиеся в вашем распоряжении по окончании работы, и помните, что ваше обязательство по защите конфиденциальных данных сохраняется после прекращения работы. **Если вам стало известно о том, что конфиденциальные данные были переданы посторонним лицам (намеренно или непреднамеренно), или ваш ноутбук или мобильное устройство были утеряны, украдены или скомпрометированы, и в них содержались конфиденциальные данные, немедленно обратитесь к руководителю отдела этики и комплаенса и ИТ-консьержу, чтобы сообщить об инциденте.**

У вас есть вопрос или проблема?

Есть много способов задать вопрос или поднять озабоченность по поводу этой политики. Выберите вариант, который вам наиболее удобно использовать. Независимо от того, какой вариант вы выберете, ваша конфиденциальность будет соблюдаться, и возмездие не будет допущено:

- Ваш руководитель или руководство следующего уровня
- Людских ресурсов
- Этика и соблюдение нормативных требований
energizercompliance@energizer.com



Глобальная политика защиты данных

Дата вступления в силу: Февраль 2018 года

Последняя редакция: Апрель 2025 года

- Правовыми
- Горячая линия Energizer: www.EnergizerHelpLine.com
 - Позвоните по телефону 1-877-521-5625 (США)
 - Дополнительные телефонные номера на www.EnergizerHelpLine.com
 - Текст «Отчет» по 314-668-1383 (только для Северной Америки)
 - вы можете остаться анонимными, если выберете
 - доступно 24 часа и управляется сторонним поставщиком

Section 5: Соответствующие политики и стандарты

Имя политики
Кодекс поведения
Политика допустимого использования информационных технологий
Политика управления записями и информацией (RIM)

Section 6: История редакций

Владелец политики будет пересматривать и обновлять эту политику по мере необходимости не реже одного раза в финансовый год.

Номер редакции	Дата вступления в силу	Собственник	Описание изменения
4	Апрель 2024 года	Seth Smoker	Обновленный владелец политики; изменен «руководитель отдела по этике и соблюдению» на «помощник Генерального юрисконсульта по вопросам глобальной этики и комплаенса» и изменен контактную информацию на Карен Бенсон
3	Март 2021 года	Ronnie Kann	Обновлена контактная информация для горячей линии Energizer
2	Ноябрь 2020 года	Ronnie Kann	Обновленный владелец политики; изменен «главный сотрудник по соблюдению» на «руководитель отдела этики и соблюдения»; добавлен способ задать вопрос или сообщить о проблеме; добавить политику RIM и Кодекс поведения в соответствующие политики и стандарты
1	Январь 2018 года	Kathy Rehmer	Новой политики



Глобальная политика защиты данных

Дата вступления в силу: Февраль 2018 года

Последняя редакция: Апрель 2025 года

Section 7: Требуемое утверждение

Подпись в файле _____

Подпись в файле _____



Política global de protección de datos

Fecha de entrada en vigor: Febrero de 2018

Última revisión: Abril de 2025

Section 1: Finalidad de esta Política

Esta Política Global de Protección de Datos (la "Política") promueve un equilibrio efectivo entre las prácticas de seguridad de la información y las necesidades empresariales, manteniendo al mismo tiempo el cumplimiento de las leyes pertinentes. La Política ayuda a Energizer a cumplir con nuestras obligaciones legales mientras mantiene la capacidad de que el negocio sea ágil y cumpla con las expectativas del cliente. Como se expone a continuación con más detalle, Energizer requiere diferentes niveles de controles de seguridad dependiendo de la clasificación de la información a proteger, que se basan en el riesgo, la practicidad y otras consideraciones.

Nuestros clientes, colegas y otros confían en nosotros para proteger su información. Una violación de la seguridad de los datos podría dañar gravemente nuestra credibilidad, causar pérdida de negocio y otros daños a las personas afectadas. Una seguridad sólida de los datos requiere diligencia por parte de todos los colegas, contratistas y cualquier otra persona que acceda o utilice nuestros activos de datos. La protección de datos es parte del trabajo de todos.

Principios rectores

Todos los colegas deben tener en cuenta los siguientes principios para la protección de datos:

- i. Energizer protege la confidencialidad, integridad y acceso a sus activos de datos.
- ii. Energizer cumplirá con las leyes de privacidad y protección de datos aplicables.
- iii. Energizer equilibra las necesidades de eficiencia empresarial con la necesidad de proteger la información personal, patentada y otra información confidencial de riesgos innecesarios.
- iv. Energizer solo otorga acceso a información personal, de propiedad y de otra índole confidencial a aquellos que necesitan saber y que están obligados a mantener la seguridad de la información.
- v. Los colegas de Energizer son la primera y mejor línea de defensa contra incidentes de seguridad de datos, y es responsabilidad de cada colega mantener las prácticas de esta Política.
- vi. La red, los sistemas y otros activos de Energizer son principalmente para fines comerciales. Excepto cuando la ley aplicable disponga lo contrario, usted no debe tener expectativas de privacidad al usar la red o sistemas de Energizer, incluyendo, pero no limitado a, la transmisión y almacenamiento de archivos, datos y mensajes.

Section 2: Propietario de la política y declaración de responsabilidad

Esta política es propiedad del Asesor Jurídico Asociado, Ética Global y Cumplimiento. Es responsabilidad de este individuo, junto con Legal, implementar, revisar anualmente y revisar esta política según sea necesario.



Política global de protección de datos

Fecha de entrada en vigor: Febrero de 2018

Última revisión: Abril de 2025

Nombre	Título	Teléfono	Correo electrónico
Karen Benson	Asesor General Asociado, Ética Global y Cumplimiento	954.593.6876	karen.benson@energizer.com

Section 3: Protección de datos personales

3.1 Recopilación y procesamiento de datos de colegas

Con el fin de dirigir su negocio de manera efectiva, Energizer necesita recopilar y utilizar cierta información personal sobre nuestros colegas. Las leyes y regulaciones globales de privacidad de datos requieren la recopilación, almacenamiento, procesamiento, intercambio, transferencia y uso adecuados de datos personales, incluidos los datos personales de colegas ("Datos personales de colegas"). Es responsabilidad fundamental de los colegas, tal como se describe en el Código de Conducta, utilizar los datos solo para el propósito que fue previsto y proteger adecuadamente estos datos.

Ciertos datos, incluidos los datos personales confidenciales y los datos personales, se recopilan de colegas (y en algunos casos candidatos a empleo), ya sea por parte de la empresa o los terceros autorizados de la empresa para administrar todos los aspectos del empleo, incluidos, entre otros: Nómina, compensación, viajes, reembolso de gastos, donaciones en línea, etc. administración de beneficios, procedimientos disciplinarios y de quejas, tiempo y asistencia, gestión de cursos de capacitación y gestión de carrera.

Cuando sea necesario para fines comerciales, y lo permita la ley, Energizer también puede acceder y almacenar correos electrónicos y documentos, incluidos currículum vitae (CV), que pueden contener datos personales o sensibles. Energizer también puede recopilar datos de colegas cuando supervisa las comunicaciones y los sistemas para proteger el negocio contra virus y malware o para garantizar el cumplimiento de las políticas, leyes y regulaciones.

3.2 Tipos de datos de colegas recopilados

3.2(a) – Datos personales

En la Unión Europea (UE) y en muchos otros países, los "datos personales" se definen ampliamente como cualquier información relacionada con una persona identificada o identificable (es decir, una persona que puede ser identificada directa o indirectamente por referencia a un nombre, número de identificación, etc.). En pocas palabras, los datos personales pueden incluir el nombre de una persona, la dirección de correo electrónico, la dirección física o similares.

3.2(b) – Datos personales sensibles

Las leyes de privacidad de datos varían según el país y algunos elementos de datos se consideran sensibles en ciertas jurisdicciones y requieren protección adicional porque el uso



Política global de protección de datos

Fecha de entrada en vigor: Febrero de 2018

Última revisión: Abril de 2025

inadecuado de estos datos puede conducir al robo de identidad. Por ejemplo, los Datos Personales Sensibles pueden incluir:

- Información de la cuenta bancaria o de la tarjeta de crédito (como el número de cuenta y el número de ruta)
- Identificación nacional, como número de Seguro Social
- Pasaporte #
- Sueldos e información sobre compensaciones conexas
- Información biométrica, sanitaria y médica
- Origen racial o étnico
- Creencias políticas o religiosas
- Afiliación sindical

3.3 Leyes de protección de datos

Muchos países han promulgado leyes de privacidad de datos que especifican los requisitos para el “procesamiento” de datos personales. El “procesamiento” puede incluir acciones tales como recopilar, usar, almacenar, alterar, divulgar, o transmitir datos personales, entre otros. Por ejemplo, el procesamiento de datos personales de ciudadanos de la UE (incluidos colegas y solicitantes) está regulado de tal manera que cualquier recopilación, procesamiento o transferencia de datos fuera de la UE (u otros estados aprobados) debe cumplir con las leyes, como el Reglamento General de Protección de Datos (RGPD) de la UE.

Cualquier transferencia de datos personales de la UE fuera de la UE --lo que incluye el acceso a los datos personales de la UE desde fuera de la UE-- requiere salvaguardias adecuadas antes de la transferencia de datos. Además, compartir los datos personales de la UE con un tercero (incluso con aquellos con los que tenemos un contrato) fuera de la UE requiere una seguridad adecuada y debe coordinarse con Legal y el Jefe de Ética y Cumplimiento.

3.4 – Sus responsabilidades para proteger los datos de colegas

Los colegas y contratistas están obligados a cumplir con todos los aspectos de esta Política que les sean aplicables. Si usted tiene acceso a Datos Personales y/o Datos Personales Sensibles, u otros datos personales basados en su rol dentro de la Compañía, es su deber implementar controles aprobados por Energizer para asegurar y proteger esos datos y limitar el acceso a los datos solo a aquellos que necesitan conocerlos y solo para fines comerciales necesarios y legítimos.

Energizer establece las siguientes pautas para colegas que accedan, guarden y/o transmiten (es decir, procesan) archivos con Datos Personales o Datos Personales Sensibles:

- i. Marque de forma visible todos los documentos, archivos o correos electrónicos que contengan Datos Personales sensibles con la siguiente marca:

“Personal y Confidencial”



Política global de protección de datos

Fecha de entrada en vigor: Febrero de 2018

Última revisión: Abril de 2025

-
- ii. Los archivos que contengan este tipo de datos solo deben guardarse en una ubicación segura como OneDrive, pero pueden almacenarse **temporalmente** en recursos seguros de la empresa, como computadoras portátiles o de escritorio, y eventualmente almacenarse en OneDrive.
 - iii. Proteja los archivos de datos personales sensibles con cifrado y / o contraseñas. Los archivos de datos personales confidenciales solo deben transmitirse mediante métodos seguros/cifrados, como el cifrado de línea de asunto, Citrix ShareFile o portales de transmisión seguros con un proveedor.
 - iv. Antes de compartir los Datos Personales de la UE y los Datos Personales Sensibles con terceros, asegúrese de que son apropiados y necesarios y póngase en contacto con los Recursos de Privacidad a continuación para asegurarse de que existen las salvaguardias adecuadas.
 - v. Recuerde bloquear su computadora si necesita alejarse de ella.
 - vi. No deje su computadora portátil a la vista, o sin seguridad, en su automóvil o habitación de hotel y no se aleje de ella en un lugar público, como un aeropuerto.
 - vii. Tenga en cuenta que incluso datos como nombres, direcciones de correo electrónico y otra información relacionada con una persona identificada o identificable pueden considerarse "Datos personales" bajo las leyes de privacidad de muchos países y pueden requerir protecciones adicionales.
 - viii. Los datos deben eliminarse de su computadora tan pronto como ya no tenga la necesidad de acceder a ellos, a menos que estén sujetos a una retención de litigios u otro programa de retención de registros.

Por último, notifique al Jefe de Ética y Cumplimiento si no está seguro de si cierta información o archivos pueden compartirse con otra parte, si tiene conocimiento de información sensible que se compartió por error o no autorizada, o si su computadora portátil o dispositivo móvil (teléfono o tableta) se perdió, robó o comprometió. Las computadoras portátiles o dispositivos móviles robados también deben ser reportados al Conserje DE TI.

Section 4: Protección de Datos Confidenciales o Propietarios de la Empresa

Datos confidenciales de Energizer

La Información Confidencial es información que puede causar daño a Energizer, sus clientes, colegas u otras entidades o individuos si se divulga incorrectamente, o información que no está disponible públicamente de otro modo. Los daños pueden estar relacionados con la privacidad de una persona, la posición estratégica de negocio de Energizer o la de sus clientes, o las responsabilidades legales o regulatorias. De acuerdo con sus roles y responsabilidades, puede tener acceso a los Datos Confidenciales de Energizer.

Ejemplos de Datos Confidenciales incluyen planes estratégicos, planes de marketing, datos financieros, listas de clientes, contratos, etc. planes de negocio, patentes no publicadas, secretos comerciales, documentación de fusiones y Adquisiciones, información sujeta a un acuerdo de confidencialidad u otra información técnica o comercial.



Política global de protección de datos

Fecha de entrada en vigor: Febrero de 2018

Última revisión: Abril de 2025

Esta Política requiere la protección de los Datos Confidenciales en el almacenamiento, la difusión y el intercambio, tanto dentro como fuera de la empresa, utilizando las salvaguardias administrativas, físicas y técnicas adecuadas de acuerdo con los riesgos que plantea el posible acceso no autorizado a los datos.

4.1 Sus responsabilidades para proteger los datos de la empresa

A menos que esté marcado de otra manera o claramente destinado a ser Información Pública, tratará toda la información/datos como si fuera Información Confidencial de Energizer, independientemente de su fuente o forma, incluyendo información electrónica, en papel, verbal u otra información.

Energizer establece las siguientes pautas para acceder, guardar y/o transmitir (es decir, procesar) archivos que contengan Datos Confidenciales de Energizer:

- Marque claramente todos los documentos, archivos o correos electrónicos que contengan Datos Confidenciales de Energizer con lo siguiente:

“Energizer Propietario y Confidencial”

- Los archivos que contengan este tipo de datos solo deben guardarse en una ubicación segura como OneDrive, pero pueden almacenarse temporalmente en recursos seguros de la empresa, como computadoras portátiles o de escritorio, y eventualmente almacenarse en OneDrive.
- Proteja los datos confidenciales con cifrado y/o contraseñas apropiadas y solo transmita mediante métodos seguros, como cifrado de línea de asunto, Citrix ShareFile o portales de transmisión seguros.
- Recuerde bloquear su computadora si necesita alejarse de ella.
- No deje su computadora portátil a la vista, o sin seguridad, en su automóvil o habitación de hotel y no se aleje de ella en un lugar público, como un aeropuerto.
- Los Datos Confidenciales deben eliminarse de su computadora tan pronto como ya no tenga la necesidad de acceder a ellos, a menos que estén sujetos a una retención de litigios u otros para cumplir con el programa de retención de registros de Energizer.
- Solo discutir los Datos Confidenciales en lugares no públicos o tomando medidas razonables para evitar ser escuchados.
- Solo escanea, distribuye, copia y distribuye Datos confidenciales en la medida necesaria, y garantiza que la parte receptora esté sujeta a un acuerdo de confidencialidad o bajo obligaciones similares de confidencialidad.

Devuelva todos los Datos Confidenciales en su posesión al final de su empleo y recuerde que su obligación de proteger los datos confidenciales sobrevive después de la terminación del empleo. **Si se da cuenta de que los Datos Confidenciales se compartieron con partes no autorizadas (intencionalmente o no), o de que su computadora portátil o dispositivo móvil se perdió, robó o comprometió y contenía**



Política global de protección de datos

Fecha de entrada en vigor: Febrero de 2018

Última revisión: Abril de 2025

Datos Confidenciales, póngase en contacto con el Jefe de Ética y Cumplimiento y el Conserje DE TI inmediatamente para informar del incidente.

¿Tiene alguna pregunta o preocupación?

Hay muchas maneras de hacer una pregunta o plantear una preocupación con respecto a esta política. Elige la opción que te sientas más cómodo usando. Cualquiera que sea la opción que elija, se respetará su confidencialidad y no se tolerarán represalias:

- Su gerente o liderazgo de siguiente nivel
- Recursos humanos
- Ética y cumplimiento energizercompliance@energizer.com
- Jurídico
- Línea telefónica de ayuda para energizadores: www.EnergizerHelpLine.com
 - Llame al 1-877-521-5625 (EE.UU.)
 - Números de teléfono adicionales en www.EnergizerHelpLine.com
 - Envíe el texto "Informe" al 314-668-1383 (solo América del Norte)
 - puede permanecer anónimo si lo desea
 - disponible las 24 horas y operado por un proveedor de terceros

Section 5: Políticas y normas conexas

Nombre de la política
Código de conducta
Política de uso aceptable de la tecnología de la información
Política de Gestión de Registros e Información (RIM)

Section 6: Historial de revisión

El propietario de la póliza revisará y actualizará esta política según sea necesario al menos una vez cada año fiscal.

Número de revisión	Fecha de entrada en vigor	Propietario	Descripción del cambio
4	Abril de 2024	Seth Smoker	Se actualizó el propietario de la política; se cambió "jefe de ética y cumplimiento" a "Asesor Jurídico Asociado, Ética Global y Cumplimiento" y se cambió la información de contacto a Karen Benson
3	Marzo de 2021	Ronnie Kann	Información de contacto actualizada para la línea de ayuda de Energizer
2	Noviembre de 2020	Ronnie Kann	Se actualizó el propietario de la política; se cambió "director de cumplimiento" por "jefe de ética y cumplimiento"; se agregó cómo hacer



Política global de protección de datos

Fecha de entrada en vigor: Febrero de 2018

Última revisión: Abril de 2025

			una pregunta o plantear una inquietud; se agregó la política de RIM y el Código de Conducta a las políticas y normas relacionadas
1	Enero de 2018	Kathy Rehmer	Nueva política

Section 7: Aprobación requerida

Firma en archivo _____

Firma en archivo _____