C-5 Information Security and Privacy Policy	
Policy Sponsor/Function:	EVP and Chief Financial Officer
Policy Owner:	Chief Information Security Officer
Effective Date:	March 30, 2018
Supersedes:	C-5 Information Protection and Privacy Policy November 2015

STATEMENT OF MONDELĒZ INTERNATIONAL POLICY

SUMMARY

As Mondelēz International does business in countries all around the world, we need to ensure we appropriately use and protect the information that we create, collect, access, share, and process to accomplish our business goals. This information may include the personal information of our employees, contractors, business partners, and consumers, as well as company confidential information, such as financial results, in-process patent filings, trade secrets, etc. collectively classified as Protected Information. Mondelēz International is committed to protecting and managing this information in compliance with applicable laws, regulations, and executive management directives. Everyone working for or on behalf of Mondelēz International is responsible for protecting information held by the company.

1. WHAT DOES THE LAW SAY?

Varying laws around the world require Mondelēz International to secure and appropriately manage our Protected Information, which includes personal information and other company confidential information. Personal information[1] is defined as ***any data that can be used directly or indirectly to identify or locate a natural person***. Examples of personal information include but are not limited to name, government-issued identifier, location data, an online identifier, biometric/other physiological information, financial information, and political affiliation[2]. Types of personal information that Mondelēz International owns or holds include details about our employees, contractors, business partners, customers, and consumers.

2. WHAT IS THE SCOPE OF THIS POLICY?

This Policy, and its related functional standards and procedures, applies to all Mondelēz International information, including Protected Information, regardless of form and retention (electronic, paper, verbal). This includes both information specified in laws and regulations, and that deemed as confidential by Company management.

3. WHO MUST FOLLOW THIS POLICY?

This policy applies to all Mondelēz International employees, contractors, suppliers, business partners, and any party conducting business with Mondelēz International who have access and/or process Mondelēz International information.

[1] also referred to as 'personally identifiable information (PII)' or 'personal data'

[2] The last three examples are often sub-categorised as Sensitive Personal Data and may be subject to greater restrictions in certain jurisdictions.

4. WHAT ARE THE COMPANY'S RESPONSIBILITIES?

Our Company's values and key outcomes of "unquestioned integrity in everything we do" and "safety of our people, products, and information" underpin all information protection-related activities, policies and standards.

INFORMATION SECURITY:

Mondelēz International adopts a risk-based approach to information security, whereby any intended use of company information should undergo a Criticality Assessment to formally classify the information and determine appropriate security control requirements. Such uses include but are not limited to technology projects such as the development of new applications, the purchase of external software, the outsourcing of services, the development of web sites, etc. The Criticality and Risk Assessment processes are described in the C-5 Policy Supplement.

Mondelēz International is committed to maintaining the confidentiality, integrity and availability of our information assets by implementing appropriate technical and organizational measures as detailed in our internal IS Security Standards, which are based on internationally accepted standards for information security management, and include key controls such as:

- Establishing and maintaining an organizational structure to provide management direction and support for information security
- Identifying and managing our information assets and risks to those assets
- Ensuring user awareness of responsibilities for protection of company information
- Protecting our core infrastructure, e.g. network perimeter security, data encryption in storage and transit, secure operating system configuration and vulnerability management
- Managing data backups and contingency/disaster recovery planning
- Managing logical and physical security of our information assets
- Managing security in vendor relationships
- Securing the end-user work environment
- Controlling changes to software and other information assets in a secure manner
- Managing information security incidents, including continual monitoring and correlation of information security events

PRIVACY:

The key principles of Mondelēz International's privacy policy are based on globally recognized privacy protection models such as the Generally Accepted Privacy Principles (GAPP) and jurisdictional regulations such as the European General Data Protection Regulation (GDPR) and other regional/national laws.

In general, Mondelēz International is committed to observing the following privacy principles for managing personal data:

PRINCIPLE	INTERPRETATION
NOTICE & CONSENT	Individuals will be provided notice of the purposes for which their personal data is collected and processed, and their implicit or explicit consent will be obtained for such collection and processing, where consent is applicable.

COLLECTION LIMITATION	Personal data collected will be limited to that strictly required by the stated purpose, and any such data will be obtained by lawful and fair means and, as appropriate, with the knowledge and/or consent of the individual.
DATA QUALITY	Personal data collected will be accurate, complete, relevant to stated purpose, and kept up-to-date.
USE LIMITATION, RETENTION & DISPOSAL	The use of personal data will be limited to the purposes identified in the notice and for which the individual has provided implicit or explicit consent. Personal data will be retained only for as long as necessary to fulfill the stated purposes or as required by law or regulations and thereafter appropriately disposed of.
SECURITY	Personal data will be protected by reasonable security safeguards against risks such as loss or unauthorized access, destruction, use, modification or disclosure of data.
DISCLOSURE TO THIRD PARTIES	Personal data will be disclosed to third parties only for the purposes identified in the notice and with the implicit or explicit consent of the individual, where consent is applicable.
INDIVIDUAL RIGHTS	The rights of individuals as provided by applicable local law will be upheld, e.g. providing individuals with access to their personal information held by the company for review, correction or update.
TRANSFERS	Transfers of personal data between legal entities, territories or countries will be carried out strictly in compliance with applicable local laws.

Mondelēz International is accountable for implementing measures appropriate to each of our locations for compliance with the above-mentioned privacy principles.
Mondelēz International is committed to following the principles of 'Privacy by Design' to ensure these measures are embedded in company processes.

5. WHAT DOES THE COMPANY EXPECT OF ME?

Mondelēz International expects you to work productively and use our information and information systems to help achieve our business goals. The Company also expects you to always protect its information in accordance with this policy, the policy supplement, and related internal standards and procedures.

All Protected Information should be handled on a strictly need-to-know and least privilege basis. If you need access to information classified as Protected Information then you are required to know and apply additional protection requirements such as the use of encryption, secure storage, limited access and distribution, use of secure passwords, and additional training. You are expected to be vigilant to ensure you carry out your official duties in a secure and compliant manner, and only use internally approved information assets for business purposes.

The company expects you to take appropriate measures to protect any company personal information that you handle and to ensure such data is not shared with any party without prior

clearance. In general, any activity you perform/are involved in that has the potential to affect individuals' right to privacy will need to comply with the privacy principles set out in this policy and any applicable privacy laws and regulations. A Privacy Impact Assessment (PIA) needs to be performed and appropriate measures to address the risks identified must be implemented. The PIA process helps you to ensure compliance with applicable privacy legal requirements. Refer to the C-5 Policy Supplement for additional information on the PIA process.

Additionally, if you notice any suspicious activity and/or loss of information (e.g. phishing emails), or you have reason to believe that personal or confidential information controlled by Mondelēz International may have been exposed to unauthorized access, lost, or repurposed without permission, you are expected to report this immediately via the appropriate internal channels as described on the Information Security & Compliance Teamsite, or by directly contacting a member of the Information Security & Compliance team, and the incident will be handled in accordance with the CYBERSECURITY INCIDENT RESPONSE PLAN.

You are expected to complete any Information Security and Privacy training modules that may be assigned to you through the company's internal Learning Management System.

6. MONITORING AND ENFORCEMENT

As permitted by law, Mondelēz International reserves the right to monitor employee communications as necessary for compliance purposes to protect the confidentiality, availability and integrity of company information.

7. REPORTING SUSPECTED MISCONDUCT

An individual should ask what to do if they are unsure and continue to ask until an answer is received. Potential or suspected policy violations or illegal activity should always be reported.

For more guidance, see our Speaking Up & Investigations Policy.

A. WHAT IF I THINK SOMEONE HAS VIOLATED THIS POLICY?

If it is believed someone is violating this Policy, this needs to be reported immediately to:

- An immediate supervisor
    - That supervisor's supervisor
    - That immediate department head
- Any Mondelēz International Legal Counsel
- Any Regional Privacy Lead
- The Chief Business Integrity Officer or your Regional Business Integrity Officer
- The Business Integrity group at: compliance@mdlz.com

Face-to-face discussions are often best, but there may be times when an individual may not feel comfortable talking to someone in person or prefer to remain anonymous. That is why the Integrity HelpLine and Integrity WebLine are available.

The HelpLine and WebLine, both operated by a third-party for the company, allow individuals to report concerns anywhere, anytime, and anonymously should they wish.

B. CAN I BE RETALIATED AGAINST FOR REPORTING A VIOLATION?

No. When you speak up and raise concerns or report wrongdoing in good faith, you are doing the right thing and Mondelēz International will not tolerate any retaliation against you. If you think someone has retaliated against you or any other employee for raising a concern, tell your Regional Business Integrity Officer, or contact the Integrity HelpLine or Integrity WebLine, as possible. Anyone who retaliates against another employee for raising a concern in good faith will face discipline, which may include termination. On the other hand, concerns or allegations raised in bad faith (e.g., knowing they are not true) will not be tolerated and employees who make them are subject to discipline, including termination of employment. For more information about "speaking up," refer to the Speaking Up & Investigations Policy.

8. WHERE CAN I GET MORE INFORMATION?

Functional Data Owners, Legal Counsels, Business Integrity, Data Privacy Officers and Information Security & Compliance (IS&C) are key resources who can provide additional information to help you better understand the requirements of this policy. These support roles and resources are defined in greater detail in the C-5 Policy Supplement.