Georgian American University, LLC

Guidelines for Employees Using Corporate Email Addresses

Contents

Introduction

This policy outlines the guidelines for email usage in the workplace in accordance with the Law of Georgia on "Personal Data Protection." All employees, contractors, and third parties

using the company's email system are required to follow these guidelines to ensure the protection of personal data and compliance with data protection laws.

Scope

This policy applies to all email communications sent or received using the company's email accounts, regardless of the device or location from which they are accessed.

General Principles

1. It is recommended to use work email accounts exclusively for work-related communications.
2. Treat all email content as important and act in accordance with the principles of consideration and integrity.
3. Exercise caution and professionalism in all email communications.

Personal Data Protection

Data Minimization

1. Process only the necessary personal data via email.
2. Avoid, whenever possible, using email to transmit special categories of personal data.
3. Where feasible, use initials or partial information instead of full names.

Purpose Limitation

1. Use personal data in emails only for the specific, legitimate purpose for which it was collected.
2. Do not use emails for purposes for which they were not intended.

Storage Limitation

1. Regularly review and delete emails containing personal data that are no longer needed.
2. Follow the company's data retention schedule for emails.

Consent and Legal Basis

1. Ensure you have a valid legal basis for processing personal data via email (e.g., consent, contract, legitimate interest).
2. For marketing emails, maintain records of recipient consent and promptly honor opt-out requests.

Transparency

When collecting and processing personal data via email, clearly state the purpose and how the data will be used, stored, and processed.

Security Measures

1. Use strong, unique passwords for email accounts.
2. Encrypt emails containing sensitive personal data.
3. Be cautious when opening attachments or clicking on links from unknown sources.
4. Log out of email accounts when not in use, especially on shared or public devices.

Recipient Confidentiality

1. Use BCC (Blind Carbon Copy) when sending emails to multiple recipients who do not need to see each other's email addresses.
2. Double-check recipient lists before sending emails containing personal data.

Rights of the Domain Owner

The domain owner has the right to retain a work email account for a certain period after an employee's departure, solely for legitimate purposes and in compliance with the law.

Data Subject Rights

1. Immediately forward any requests from data subjects regarding their personal data (e.g., access, correction, deletion) to the Data Protection Officer (DPO).
2. Do not disclose personal data via email without verifying the requester's identity and consulting the DPO.

Incident Response

1. Report any suspected incident (e.g., sending personal data to the wrong recipient, account compromise) to the IT department and the DPO immediately.
2. Do not attempt to resolve data breaches independently without proper guidance.

Data Transfers

1. Exercise caution when sending personal data to recipients outside the scope defined by Georgian legislation.
2. Consult the DPO before transferring personal data internationally via email.

Email Retention and Deletion

1. Retain emails only as long as necessary for the purpose they were sent or received.
2. Delete or archive emails in accordance with the company's retention policy.
3. Regularly empty the "Trash" folder.

Monitoring and Enforcement

1. The company reserves the right to monitor email usage to ensure compliance with this policy.
2. Violations of this policy may result in disciplinary action, up to and including termination of employment.

Policy Review

This policy will be reviewed and updated as necessary to ensure continuous compliance with the Law of Georgia on "Personal Data Protection" and other relevant data protection laws. For questions regarding this policy, please contact the Data Protection Officer.