



# Data Privacy Overview – IEEE Technical Activities

*February 2022*

# Agenda

- ▶ Data Privacy Overview
- ▶ Current state of IEEE and TA data privacy activities
- ▶ Critical Areas for Staff and Volunteers
  - Handling of Data Breaches (process review)
  - Handling of Data Subject Requests (process review)
- ▶ Next Steps
- ▶ How you can help

# Our Current View of Data Privacy Began with GDPR

- ▶ The European Union General Data Protection Regulation (GDPR) (Regulation EU-2016/679) is a regulation by which the European Parliament, the Council of the European Union, and the European Commission intend to strengthen and unify data protection for all EU citizens and individuals within the European Union (EU)
- ▶ The GDPR's primary aim is to give control back to citizens and residents over their personal data. Because of its extraterritorial aspects, international businesses are impacted by the regulation
- ▶ The GDPR applies to organizations established in the EU and to organizations, whether or not established in the EU, that process the personal data of EU individuals
  - IEEE meets these qualifications and is subject to the GDPR and has committed to support data privacy
- ▶ Went into effect on **25 May 2018**. Additional similar regulations have also been enacted since then



## What are Some of the Key Points?

- ▶ **Right to be Forgotten:** Individuals may require data controller to erase their personal information from databases.
- ▶ **Right to Access/Data Portability:** If asked, an organization must provide a copy of personal data in a commonly used and machine-readable electronic format.
- ▶ **Breach Notification:** Organizations are now required to report data breaches to regulatory authorities within 72 hours of first becoming aware of the breach.
- ▶ **Privacy and Data Considerations:** Organizations must design systems with privacy in mind from the outset (“Privacy by Design”). Organizations also should only process and maintain the data necessary for the completion of their duties, as well as limit access to only those needing this information.

**Fines for non-compliance may be substantial**



## Consent as a Basis for the Use of Personal Information

- ▶ The GDPR and other data privacy regulations allows for the processing of personal data under specific circumstances; one is if the individual has provided consent
  - Consent must be opt-in, implied consent/opt-out is no longer viable
  - Consent to use personal data must be “freely given, specific, informed, and unambiguous”
- ▶ Organizations must request consent in an intelligible and easily accessible form; legalese terms and conditions will not be acceptable
- ▶ If personal data will be shared with third parties, this must be disclosed to gain effective consent
- ▶ Consent must be as easy to withdraw as it is to give

## IEEE Actions Addressing Data Privacy

- ▶ Updated compliance training courses for IEEE staff and volunteers
- ▶ Evaluated existing vendor service agreements to ensure inclusion of data privacy-related terms and conditions
- ▶ Evaluated business platforms and applications such as conference registration systems, websites, peer review tools, marketing and customer management systems to assess data privacy concerns
- ▶ Improved consent and opt-out capabilities and centralized record keeping to enable customers to manage communications
- ▶ Moving towards centralized applications and services where possible



# What Does This Mean to IEEE Volunteers and Staff?

- ▶ Compliance relies on all of IEEE, both volunteers and staff
  - Consent-based marketing and communications is critical
  - Data must be handled properly
    - New Data Access and Use Policy
    - Updated Records Management Program
- ▶ Processes for collecting personal data and emailing on behalf of IEEE have changed. This may include deletion of data currently in your possession
- ▶ New tools and processes developed to support compliance
  - Data Subject Requests
  - Capture, tracking and application of consent of personal data use
- ▶ Data breaches are critical and must be reported immediately by staff or volunteers



# Technical Activities GDPR Bulletins

<https://ta.ieee.org/operations/technical-activities-data-privacy-resource-page>

- ▶ Bulletin #1 – Overview of EU-GDPR and other Data Privacy Regulations
- ▶ Bulletin #2 – Handling Data Breaches
- ▶ Bulletin #3 – Data Privacy Consent Permission Marketing
- ▶ Bulletin #4 – Data Privacy and Working with Event Contractors and Vendors
- ▶ Bulletin #5 – Complying with Data Privacy During the Event Registration Process
- ▶ Bulletin #6 – Handling Requests From Individuals under GDPR and other Data Privacy Regulations
- ▶ Bulletin #7 – GDPR and Data Privacy Terms
- ▶ Bulletin #8 – Social Media & Data Privacy
- ▶ Bulletin #9 – Data Privacy and Personal Information on Websites
- ▶ Bulletin #10 - Consent Capture and Recording in the IEEE Consent Management System
- ▶ Bulletin #11 – Mailing List Consent Validation



# Links to Additional Resources

<https://ta.ieee.org/operations/technical-activities-data-privacy-resource-page>

- ▶ [IEEE Data Access and Use Policy](#)
- ▶ [Training](#)
- ▶ [FAQs](#)
- ▶ [GDPR Dictionary](#)
- ▶ [GDPR Quick Facts](#)
- ▶ [IEEE Marketing Outreach Guidelines](#)
- ▶ [IEEE Website and Campaign Consent Collection Instructions](#)

# Collection and Use of Consent

- ▶ Collection of consent (input to IEEE Content Management System (CMS))
  - Acceptance of IEEE Privacy Policy populated by:
    - Capture on IEEE websites
    - Capture via email marketing campaign
    - Capture via event registration using Bulk List Loading process or direct feed to the CMS
  - Website capture modules developed and waiting on technical instructions from IT
  - General marketing consent captured on websites or campaigns feed to the CMS
  - [Bulletin #10: Consent Capture and Recording in the IEEE Consent Management System](#)
- ▶ Validation prior to marketing communications (use of consent)
  - Validation of mailing lists requires screening against the CMS to ensure agreement and confirm any “Do Not Contact” status
    - For internally managed campaigns, validation occurs automatically
    - Third party campaigns and other external lists require manual validation using the List Validation Tool
  - [Bulletin #11: Mailing List Consent Validation](#)



# When to Use the List Validator Tool

|                    |   |   |  |
|--------------------|---|---|--|
| <b>List Source</b> | <b>External</b><br>(Obtained from Non-IEEE Owner) | <b>Use List Validator</b>   | <b>Use List Validator</b>  |
|                    | <b>Internal</b><br>(Siebel, Tableau)              | <b>List Validator Not Required</b>  | <b>List Validator Not Required</b>                                   |
|                    |   | <b>Internal, integrated</b><br>(e.g., Tableau, eNotice, enterprise<br>Marketo, BDRS Services) | <b>External, standalone</b><br>(e.g., MailChimp,<br>ConstantContact) |

## Campaign Tool, Service



# Marketing Rules of Engagement Summary

## ▶ List management

- Valid audiences based on interactions, purchases or engagement
- Maintain clean lists
- Remove invalid emails, local “Unsubscribes”, or names that have had no interaction in the past two years

## ▶ Campaign management options

- Internal resources (BDRS, Marketo, eNotice)
- External third-party vendors (e.g. MailChimp, ConstantContact, Higher Logic (previously MagnetMail))

## ▶ Email practices

- All communications MUST have a functioning “Unsubscribe” option
- Inclusion of acceptance of the IEEE Privacy Policy

- ▶ For additional information see the [IEEE Marketing Outreach Guidelines](#) and the [TA Bulletin #3 – Data Privacy Consent Permission Marketing](#)



# Events and Data Privacy

## *Attendee Registration*

- ▶ Each event registration must collect consent locally to the following prior to processing the registration:
  - IEEE Privacy Policy
  - IEEE Event Terms & Conditions
- ▶ Upon conclusion of the event, attendee registration lists with the appropriate acceptances must be submitted to IEEE for inclusion in IEEE's Content Management System (CMS)
  - Direct feed from Cvent registration system, managed by MCE
  - Bulk List Load process
- ▶ Onsite registration should take action to protect registrant data:
  - Verify that the individual picking up a name badge is the actual individual
  - Shred any uncollected name badges
  - Lock registration laptops at all times
  - Avoid printing any registrant lists and shred those printed when no longer needed
- ▶ For additional information, see the [TA Data Privacy Bulletin #5: Complying with GDPR During the Event Registration Process](#)



# Personal Information on Websites

## ▶ Website Guidelines

- Volunteer leadership groups (Society AdCom, ExCom, Committees)
    - Only provide the information needed to allow other community members to contact them during their current term
    - Acceptable information includes; name, email, photo. Affiliation or employer should only be included when that is required information
    - Do NOT include address (home/work) and phone numbers
    - When an individual's term expires, the email address should be removed from the website
  - Reviews or Testimonials
    - May be in written or video format
    - May include name, likeness and IEEE affiliation, but no contact information is appropriate
    - Should obtain agreement from the individual to use their image or video, comments, and opinions
  - Awards or Honors Recipients
    - Provide only the name of the individual, no contact information
    - Only include affiliation if it is relevant to the nature of the recognition
    - Photos of the award presentation are appropriate
- ▶ For complete information, see [Technical Activities GDPR Bulletin #9 – Personal Information on Websites](#)



# IEEE Data Access and Use Policy

## *Policy Summary*

- ▶ This [policy](#) outlines the data privacy responsibilities of IEEE Staff and Volunteers, as well as associated third parties acting on behalf of IEEE, when collecting and/or managing personal data
- ▶ Data Collection and Access
  - Must present to data subjects the purpose for which the data is being collected, a link and agreement to the IEEE Privacy Policy, a link to any specific terms and conditions and a link to agree to receive additional information outside of the purpose described (subscriptions)
  - These agreements/acceptances must be communicated to IEEE CMS for tracking and compliance during marketing activities
  - Publication or sharing of data must be in accordance with the IEEE policies and practices
  - Mass email communications must allow the user to unsubscribe from further communications
- ▶ Data Processing and Handling
  - IEEE is responsible for all IEEE Data processed on his behalf, including that done by third party partners
  - Data shall only be processed as previously communicated to the user when the data was given
  - Processing the data is necessary for legitimate business purposes; or there are legal requirements for processing the data (e.g. processing a financial transaction during a purchase)



# IEEE Data Access and Use Policy – cont.

## ▶ Data Management

- Sensitive personal data must be encrypted
- Must take precautions to make sure IEEE Data is stored and handled securely and is not accessible to unauthorized individuals
- Data is deleted from personal devices where it is no longer needed
- See the updated Records Retention schedule for when to keep data and when to delete it

## ▶ Data Privacy [compliance course](#) for volunteers and staff

- Updated with information about the new policy



# Handling Data Breaches Under GDPR

- ▶ Data Breach protocol documented and communicated in [TA GDPR Bulletin #2: Handling Data Breaches under GDPR](#)
  - Simple description of what a breach could entail
  - Emphasis on rapid action to notify IEEE
  - Directed to report to IEEE IT Security Team at [privacy@ieee.org](mailto:privacy@ieee.org)
  - Recommended to forward bulletin to colleagues who handle personal data, newsletters/websites or other activities that include personal data
- ▶ Data Breach protocol also included in the [Data Access and Use Policy](#) and associated training
- ▶ Breaches are anything that potentially exposes sensitive information
  - Hacking or system intrusions
  - Loss or theft of PC, mobile device
  - Sending personal data to an incorrect recipient
  - Access by an unauthorized third party



# Types of Data Subject Requests

*Putting control of personal information in the hands of the data subject*

- ▶ Right of access ('Right to know what information has been collected')
- ▶ Right to rectification ('Right to correct or update data')
- ▶ Right to erasure ('Right to be forgotten')
- ▶ Right to restriction of processing ('Exclude my data from defined processing')
- ▶ Communicate any rectification or erasure of personal data or restriction of processing
- ▶ Right to data portability
- ▶ Automated individual decision-making, including profiling

These requests apply to **ALL** areas where data is held or processed, including staff, volunteer, and third-party partners



# Handling Data Subject Requests - Overview

- ▶ Data Subject Request intake process
  - Individual requests submitted via web form, IEEE Contact Center, or by sending an email to Privacy mailbox with specific subject-line
  - Requests evaluated by DPO and Legal to determine legitimacy
  - Requests passed to OUs for action
- ▶ Technical Activities process developed in July 2018 for outreach to S/C/TC for action and verification ([TA GDPR Bulletin #6: Handling Requests From Individuals Under GDPR](#))
- ▶ Notification to S/C/TC primary contacts for action
  - Executive office staff (ED or designate) or other TA staff (39 communities)
  - Third-party association support vendor (e.g., ConferenceCatalyst) (11 communities)
  - For volunteer-only societies, default is President who may delegate to POC (18 communities)
- ▶ Process improvements identified and being developed
  - Separate process for conferences with direct outreach by MCE required and under development
  - Focus on positive confirmation of action by POCs to ensure compliance
  - Annual update to POC list in January



# Society/Council/TC Data Subject Request Point of Contact

## *Roles and Responsibilities*

- ▶ Responsible for checking all relevant systems for the data subject's information for each type of request that is issued
  - Marketing lists
  - Activity participants (conference/events, webinars, training or certification programs, publishing, etc.)
- ▶ Some lists are reviewed by other IEEE organizations and do not need to be checked by the S/C/TC
  - Membership information will be handled by MGA
  - Centralized training and education are handled by EA
  - Periodical authors/reviewers in ScholarOne are handled by the Publications team
  - Centralized marketing-held lists such as BDRS, Marketo
- ▶ Request type and action
  - Right to be Forgotten - Removing and confirm removal of data subject from relevant systems
  - Access to Their Data - Providing data file for each instance the data subject appears
  - Retract Consent from Communications - Removing and confirm removal of data subject from relevant systems



# How You Can Help

- ▶ IEEE Volunteers and Staff should familiarize yourself with data privacy information
  - TA Data Privacy Bulletins
  - Permission-based marketing approach
  - Tools (bulk list load, list validation, etc.)
  - New Data Access and Use Policy
- ▶ Reach out to the GDPR team to respond to questions you can't answer via [TA Answer Central](#)
- ▶ Be responsive to Data Subject Requests
  - Investigate and act promptly
  - Respond back to the TA Coordinator via the email instructions
- ▶ Communicate importance and process for volunteers to report data breaches right away



# Data Privacy Resources

- ▶ IEEE Policies
  - [IEEE Privacy Policy](#)
  - [IEEE Data Access and Use Policy](#)
  - [IEEE Social Media Policy](#)
  - [IEEE Data Retention Guidelines](#)
- ▶ Key Tools and Resources
  - [IEEE Privacy Portal](#)
  - [Bulletin #4: Data Privacy and Working with Event Contractors and Vendors](#)
  - [Bulletin #5: Data Privacy and Event Registration](#)
  - [Bulletin #10: Consent Capture and Recording in the IEEE Consent Management System](#)
  - [Bulletin #11: Mailing List Consent Validation](#)
- ▶ [IEEE Volunteer GDPR Dashboard](#)
- ▶ [TA Operations Resource Page](#)
- ▶ [TA Answer Central](#)

