GDPR - General Data Protection Regulation

- briefly

IEEE EMC Society Privacy Chair
Susanne Kaule
July, 22 2019 IEEE EMC SIPI, New Orleans, USA

EMC SOCIETY

IEEE
Advancing Technology for Humanity

Agenda

- GDPR Overview
- Current state of IEEE and TA GDPR 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

What is the GDPR?

- The 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***

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 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

What IEEE Has Done to Address GDPR

- Updated compliance training courses for IEEE staff and volunteers
- Evaluated existing vendor service agreements to ensure inclusion of GDPR-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
- Moving towards centralized applications and services where possible
- Improved consent and opt-out capabilities and record keeping to enable customers to manage communications

What Does This Mean to IEEE Volunteers and Staff?

- GDPR 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 (pending approval by IEEE Board of Directors in June 2019)
  - Data breaches are critical and must be reported immediately
- 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

The IEEE GDPR team recognizes and values the contributions of our volunteers and is committed to ensuring that they are able to perform their role in a compliant manner

Technical Activities GDPR Bulletins

https://ta.ieee.org/operations/technical-activities-gdpr-resource-page

- Bulletin #1 – Overview of the EU General Data Protection Regulation (13 June 2018)
- Bulletin #2 – Handling Data Breaches under GDPR (18 June 2018)
- Bulletin #3 – GDPR Communication Guidelines (18 July 2018, *re-issue in development*)
- Bulletin #4 – GDPR and Working with Event Contractors and Vendors (19 July 2018)
- Bulletin #5 – Complying with GDPR During the Event Registration Process (24 July 2018)
- Bulletin #6 – Handling Requests From Individuals under GDPR (31 July 2018)
- Bulletin #7 – GDPR Terms (6 September 2018)
- Bulletin #8 – Social Media & GDPR (3 October 2018)
- Bulletin #9 – Personal Information on Websites (22 October 2018)

Additional TA GDPR Bulletins - Planned

Bulletin	Information
Bulletin #10 – Identifying New Audiences	When and how to grow your target market
Bulletin #11 - IEEE List Validation Tool	When and how to use the tool
Bulletin #12 - IEEE Consent Bulk Upload Tool	When and how to use the tool
Bulletin #13 - GDPR Training Resources Available	List of training information available to staff and volun
Bulletin #14 - IEEE Staff and Volunteer Responsibilities	Summary of the Data Use policy guidance (Dependenc policy approval)
Bulletin #15 - Dealing with Vendors to Ensure GDPR Compliance	Contracting process to ensure that all vendors are GDI compliant
Bulletin #16 – List Management	Best practices for list management
Bulletin #17 – Campaign Management	The proper way to conduct a marketing campaign
Bulletin #18 – IEEE Consent Capture	When and how to deploy the capture tool for websites campaigns

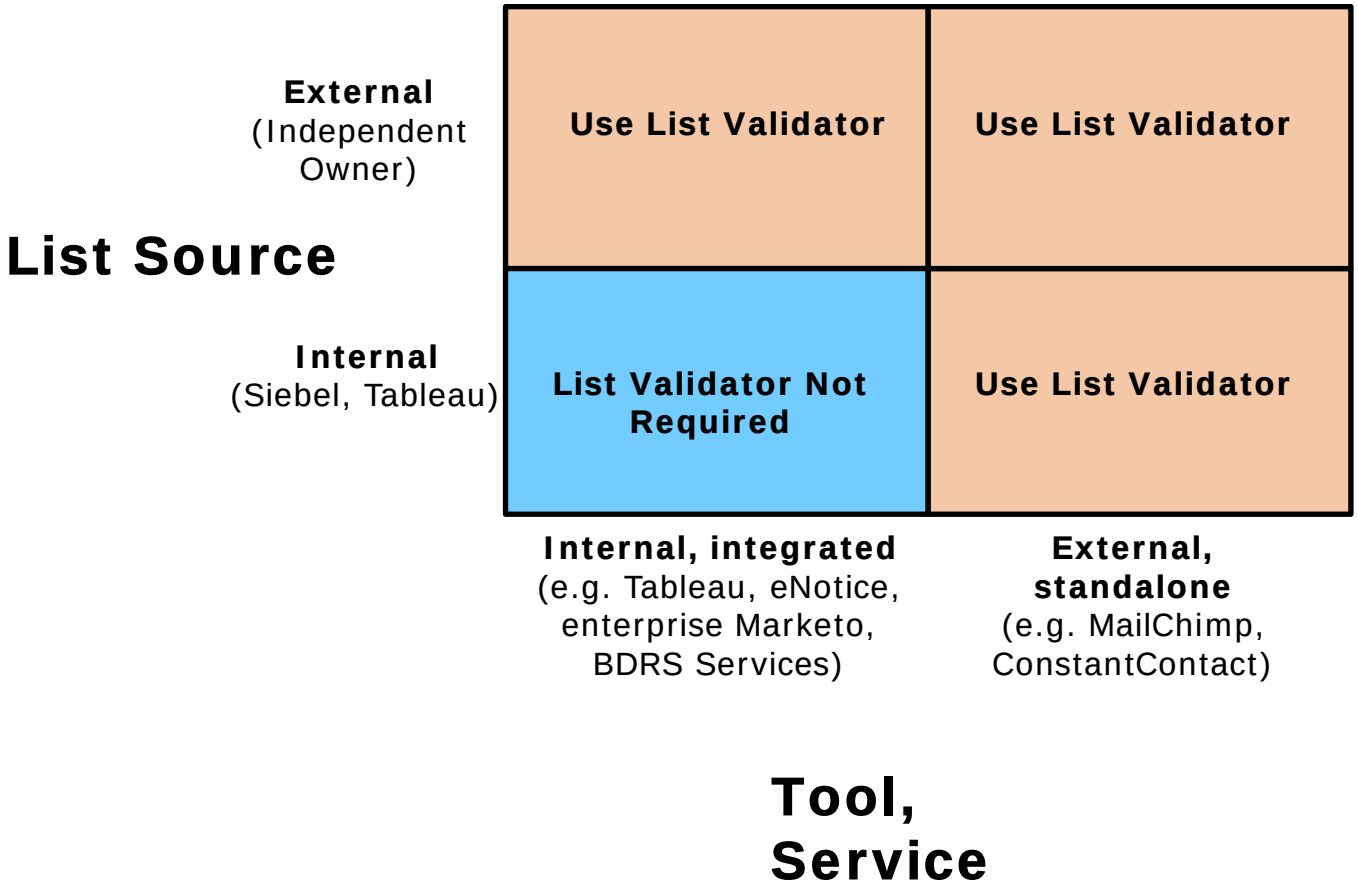
Key Points for IEEE Staff and Volunteers

- Consent is critical to ongoing compliant-based marketing activities
- Data must be handled properly
  - New Data Access and Use Policy (pending approval by IEEE Board of Directors in June 2019)
- Data breaches are critical and must be reported immediately
- We must honor the rights of our customers in handling personal data

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 tool or direct feed to the CMS
  - Website capture modules developed and waiting on technical instructions from IT
  - Marketing guidance on when/where to use under development (TA team)
- 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
  - Marketing guidance on using Validation will be released in ***Bulletin #11 - IEEE List Validation Tool***

When to Use the List Validator Tool



Marketing Rules of Engagement Summary

- List management
  - Valid audiences based on interactions, purchases or engagement
  - Keep lists clean
  - 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 (was MagnetMail))
- Email practices
  - All communications MUST have a functioning “Unsubscribe” option
  - Inclusion of acceptance of the IEEE Privacy Policy
- Communications plan
  - Updated TA Bulletins

Events and GDPR

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) via the Bulk List Load Utility unless registration system directly linked to the CMS
  - Lists submitted by events to TA contact person for loading into the CMS (Bulk Consent Load tool)
- 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

Personal Information on Websites

- Going forward the following guidelines must be adhered to:
  - 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 (https://ta.ieee.org/operations/technical-activities-gdpr-resource-page)

IEEE Data Access and Use Policy

Policy Summary

- This policy outlines the responsibilities under GDPR 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
- Final IEEE BoD approval scheduled for June 2019
- Data Privacy compliance course for volunteers and staff
  - Updated with information about the new policy
  - Initial rollout to Volunteer leadership in February 2019
  - Additional wave rolling out fall 2019 to other volunteer positions who collect/process personal data

Update to the IEEE Records Management Program is also underway

Handling Data Breaches Under GDPR

- Data Breach protocol documented and communicated in TA GDPR Bulletin #2: Handling Data Breaches under GDPR (18 June 2018)
  - 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
  - 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
  - Will re-communicate process when DA&U Policy is approved (review by BoD at June meeting)
- 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 un-authorised 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 is present')
- Right to rectification (data cleanup/correction)
- 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 initial intake process**
  - Request sent via email to Privacy mailbox with specific subject-line
  - Evaluated by DPO and Legal to determine legitimacy
  - Request passed to OUs for action
- **Technical Activities process developed in July 2018 for outreach to S/C/TC for action and verification**
- **Notification to S/C/TC on handling requests**
  - TA GDPR Bulletin #6: Handling Requests From Individuals Under GDPR (31 July 2018)
  - Direct communication to S/C Presidents, copy to society Executive Directors (sent 13 July 2018 under Kathy Land signature, re-sent under Ray Liu signature in April 2019)
- **Establishment of responsible point person for each community (new addition)**
  - 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 implemented**
  - More direct staff engagement as Points of Contact (POC) for S/C/TCs
  - Separate process for conferences with direct outreach by MCE required and under development
  - Focus on positive confirmation of action by POCs to ensure compliance
  - Re-confirmation of volunteer responsibilities to take place each December
  - Annual update to POC list in January

Society / Council / TC GDPR Point of Contact (PoC)

Roles and Responsibilities

- Responsible for checking all relevant systems for the data subject's information for each type of request that is issued
  - Membership
  - S/C/TC events, webinars, etc. other than technical conferences
  - Publications
  - Other systems as available
- 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

ED, and/or Staff, or OU President/delegate

Overall TA Next Steps

- Execute on training, education and communication plans over the coming months
  - Additional TA GDPR Bulletins
  - New webinars and updated TA GDRP Resource Page on TA Ops website
  - Leadership training in November
- Finalize process improvement for handling conference DSRs
- Roll out Consent Capture process for websites
- Update PIA/DPIA information inventory in new tool (significant work effort)
- Develop process for responding to Data Subject Requests for Conferences

How You Can Help

- Familiarize yourself and your key volunteers on GDPR information
  - Bulletins
  - Permission-based marketing approach
  - Tools (bulk load, list validation, etc.)
  - New Data Access and Use Policy (approval by BoD in June)
- 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 take action promptly
  - Respond back to the TA SME
- Communicate importance and process for volunteers to report data breaches right away

GDPR Resources

- Policy Updates and Developments
  - IEEE Privacy Policy (Updated) https://www.ieee.org/security-privacy.html
  - IEEE Data Access and Use Policy (approval by IEEE BoD pending)
  - IEEE Social Media Policy https://brand-experience.ieee.org/guidelines/digital/social-media/
  - IEEE Data Retention Guidelines (Update underway)
- Key Tools and Resources
  - IEEE Privacy Portal where end-users can manage their communication preferences (in limited release)
  - Bulk Loading utility for adding captured consent for events and other activities (in limited release)
  - List Validation utility for verifying marketing lists against policy acceptance and subscriptions (in limited release)
- IEEE Volunteer GDPR Dashboard: http://sites.ieee.org/gdpr/
- TA Operations Resource Page: https://ta.ieee.org/operations/technical-activities-gdpr-resource-page
- TA Answer Central: https://ta.ieee.org/home/ta-answer-central

What needs to be done

- Custom fit the IEEE Guide for the EMC Society
- Inform chapter chairs to apply the IEEE EMC Society Guide for GDPR compliant event organization
- How can we “control” that the chapters are implementing the GDPR compliant event organization ?

What needs to be done

- In general: Records of processing activities
- Break down to chapter responsibilities – BOD can provide form which needs to be filled out by single chapters
- but, no information to be found from IEEE side
- Stay informed – Bulletins of IEEE TA Operations

EMC SOCIETY

IEEE Advancing Technology for Humanity

Thank you for your attention

EMC SOCIETY

IEEE
Advancing Technology for Humanity

Sources:

- https://edps.europa.eu
- https://gdpr-info.eu/
- https://eugdpr.org/the-regulation/
- https://ta.ieee.org/operations/technical-activities-gdpr-resource-page
- https://ta.ieee.org/operations/gdpr-dictionary
- https://www.ieee.org/security-privacy.html
- http://sites.ieee.org/gdpr/

EMC SOCIETY

IEEE
Advancing Technology for Humanity