

# General Data Protection Regulation

## GDPR

### MS Ireland Privacy Statement

MS IRELAND is committed to protecting the privacy of people who use our services, employment candidates and current employees, contacts, fundraisers, business partners, and other third parties we deal with, such as family members. This Privacy Statement details how MS IRELAND collects, uses, discloses, transfers and stores your personal information. It applies to personal data about you that we collect, use and otherwise process in connection with your relationship with MS IRELAND.

MS Ireland's Privacy Statement is available on

<https://www.ms-society.ie/pages/what-we-do/about-us/terms-conditions-and-privacy>

### What Branches need to do to Ensure Consent?

- ❖ **Letters/writing by post** - you give your contacts the option to **opt out** of correspondence from the Branch at the end of your letter
- ❖ **Texts, emails and newsletters** – contacts have to **opt in** to receive any content from the Branch

### Branches must ensure data is secure

- Branch data is used only for the purposes of the Branch to function locally.
- Record where the data came from i.e. from attendance at a physio class or at the yoga sessions or coffee morning etc.
- The data needs to be kept safely and securely.
- The Branch should keep hard copy personal data and sensitive and confidential information securely locked away in a filing cabinet.
- All Branch data and documents relating to **Financial Assistance** should be stored in **The Regional Offices**
- It should be names and contact details **ONLY** kept by the Branch
- Ensure that all Branch smart devices and computer equipment have secure passwords.
- When using Branch smart devices or computer equipment ensure that no other person (or CCTV) can view your work screen.
- Lock your Branch smart devices and computer equipment in the boot of your car, where possible when you are travelling.
- Unless you can do so securely and it is absolutely necessary for work purposes, do not take USB or portable storage devices containing personal data, sensitive or confidential data out of a secure environment.

## General Data Protection Regulation

# GDPR

- Do not read Branch-related hard copy documents and files containing personal data, sensitive or confidential information in a public place where they can be overseen by others or CCTV.
- Always conduct Branch meetings in private rooms where Branch business cannot be overheard.
- Always check a meeting room or meeting place for Branch-related hard copy documents and files before you leave a meeting location. Don't risk leaving documents behind!
- Check hard copy documents before discarding them in rubbish bins. Shred sensitive or confidential information.
- Check an email before you click 'Send' and 'Reply All'. Is there sensitive or confidential information contained in the email or attachments, including in previous emails in a chain of correspondence?
- Always BLIND cc recipients in your email if you are sending the email to more than one person. Email addresses cannot be available to view by others.
- Check social media posts before uploading or commenting. If you post sensitive or confidential data online, you may have no control over who views the information.