International Labour Organization | ACT/EMP

Data confidentiality and protection

Any information that an Employer or Business Membership Organization stores needs to be properly protected, whether it be digital data or traditional hard copies. In an increasing number of jurisdictions, data usage is protected by law, everything from financial information and payment details to contact information of staff and members. This is to prevent that data being misused by third parties. But there are also compelling reasons for an EBMO to ensure high standards of data confidentiality and protection aside from legal liabilities and compliance.

Individual negligence, intentional misconduct or security breaches resulting from poor data security could damage trust or confidence in the EBMO or result in negative repercussions for individual staff or members. Given data is a strategic asset, integral to the core value proposition of any EBMO, its protection is also vital to innovation and competitive advantage.

What data needs to be protected?

Common data that EBMO might store includes names of staff and members; address and contact information of staff and members; bank account details of staff and members; health information of staff; minutes of meetings; records on member participation in activities and services; and survey or research findings collected to support policy advocacy;

Putting appropriate safeguards in place - Some general considerations for EBMO:

- Ensure clear and appropriate direction is provided in the constitution and bylaws on the stewardship of data;
- Confidential data should be marked “Confidential”; have a limited, need to now distribution; be protected with advanced security features (like a password protected files); and be encrypted when being shared;
- Sensitive data should be marked “Sensitive”; have a limited, need to now distribution; and be protected when being stored (like a password protected folders or devices);
- For any members data to be made available to 3rd parties, EBMO should obtain specific consent from each member first;
- Members should be allowed to opt-in in terms of what data is made available to 3rd parties (not opt out) and should be given the option of not having their data circulated;
- EBMO should seek reconfirm consent for data sharing on a regular basis, ideally once a year upon renewal of membership subscriptions;
- Even though consent is given at one point in time there should be a right for members to withdraw this consent at any future time, including the day after it has been shared with a 3rd party.
- EBMO need clear authority and a mechanism to action the withdrawal of data from 3rd parties if a member withdraws their consent;
- EBMO have a responsibility to ensure that data is accurate. If a member changes their contact details after the data has been shared with a 3rd party, EBMO will need provisions to ensure that the information is updated and that inaccurate data is not available to other parties/in circulation;
- EBMO need to ensure there is a clear agreement with 3rd parties on what they can or can’t do with any data shared, for example, ensuring they do not pass or sell the data to other parties. A best practice is to insist on a non-disclosure agreement that sets out the terms and conditions data is shared;
- EBMO need to ensure that data is not held for longer than is needed and is deleted or destroyed once so – hard copies of confidential or sensitive information should be shredded or incinerated while data on desktops, laptops. smart phones or removable media (i.e. USB or SIM card) should be physically destroyed or wiped before disposal;

For more information on ACT/EMPs work on data as a strategic asset for EBMO visit:
https://www.ilo.org/asia/projects/WCMS_757375/lang--en/index.htm