CENTER FOR DIGITAL DEMOCRACY

Consumer Advocates, Digital Rights, and Civil Rights Groups Call on U.S. Companies to Adopt the Requirements of the General Data Protection Regulation (GDPR) in the U.S. and Worldwide

Companies processing[1] personal data in the U.S. and/or worldwide and which are subject to the GDPR in the European Union, ought to:
- extend the same individual privacy rights to their customers in the U.S. and around the world;
- implement the obligations placed on them under the GDPR;
- demonstrate that they meet these obligations;
- accept public and regulatory scrutiny and oversight of their personal data practices;
- adhere to the evolving GDPR jurisprudence and regulatory guidance.

[1] Processing under GDPR includes collecting, storing, using, altering, generating, disclosing, and destroying personal data.

Specifically, at a minimum, companies ought to:

1. **Treat the right to data privacy as a fundamental human right.**
    a. This right includes the right to:
        i. Information/notice
        ii. access
        iii. rectification
        iv. erasure
        v. restriction
        vi. portability
        vii. object
        viii. avoid certain automated decision-making and profiling, as well as direct marketing
    b. For these rights to be meaningful, give individuals effective control over the processing of their data so that they can realize their rights, including
        i. set system defaults to protect data
        ii. be transparent and fair in the way you use people's data

2. **Apply these rights and obligations to all personal data including to data that can identify an individual directly and indirectly.**

3. **Process data only if you have a legal basis to do so,** including
    a. On the basis of freely given, specific, informed and unambiguous consent
    b. If necessary for the performance of a contract

4. **In addition, process data only in accordance to the principles of fairness, transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity and confidentiality/security.**

5. **Add extra safeguards, including explicit consent, when processing sensitive personal data (such as data about ethnic or racial origin, political opinions/union membership, data concerning health, sex life or sexual orientation, genetic data, or biometric data) or data that reveals sensitive personal data, especially when using this data for profiling.**

6. **Apply extra safeguards when processing data relating to children and teens, particularly with regard to marketing and profiling.**

7. **Be transparent and accountable, and adopt technical and organizational measures to meet these obligations, including**
    a. Provide for algorithmic transparency
    b. Conduct impact assessments for high risk processing
    c. Implement *Privacy by Design and by Default*
    d. Assign resources and staff, including a Data Protection Officer
    e. Implement appropriate oversight over third party service providers/data processors
    f. Conduct regular audits
    g. Document the processing

8. **Notify consumers and regulatory authorities in case of a breach without undue delay.**

9. **Support the adoption of similar requirements in a data protection law that will ensure appropriate and effective regulatory oversight and enforcement for data processing that does not fall under EU jurisdiction.**

10. **Adopt these GDPR requirements as a baseline regardless of industry sector, in addition to any other national/federal, provincial/state or local privacy requirements that are stricter than the requirements advanced by the GDPR.**