

TDC Group's policy for data ethics and responsible handling of customers' personal data

TDC has developed a company policy for handling of customers' personal data. The policy supplements TDC's 10 rules for treatment of personal data, outlined in the "Think before you Type".

1. Respect for TDC's customers and employees' privacy is a fundamental value for TDC.
2. TDC considers data ethical concerns more far-reaching than mere compliance with and adherence to legislation.
3. TDC seeks to develop a "positive error culture" among employees, where openness about errors and problems leads to improvement.
4. TDC prioritizes openness and transparency around the on-going challenges presented by personal data and privacy, in order for companies, organizations and authorities to learn from each other's experiences.
5. Employees who handle or access customers' personal data have signed a confidentiality agreement as part of their employment contract with TDC and have received e-learning education on proper handling of personal data.
6. TDC complies with the Telecom Act's requirement to deliver public directory information, but does not resell confidential or sensitive personal information.
7. TDC only shares customer data with authorities if stipulated by law or a court decision. Emergency or national security situations constitute exceptions.
8. Machine learning, artificial intelligence and use of algorithms shall be used to support TDC's self-help options, and improve services for TDC's customers.

Detailed explanations of each policy are outlined below:

1. Respect for customers and employees' privacy is a fundamental value for TDC.

- In situations where privacy has to be balanced in relation to other reasonable concerns, privacy should be given preference. In circumstances where privacy cannot receive the highest priority, for instance as a consequence of legal- or security constraints, these instances should be reported to TDC's leadership.
- All new commercial developments with significant implications for privacy and processing of personal data have to be approved by TDC's management, which has the ultimate legal, fiduciary and data ethical responsibility for the company.

- TDC safeguards the handling of our customers' personal data and ensures that this data is not stored for a longer period of time than necessary, in relation to technical, functional and legal purposes for data storage.

2. TDC views data ethical considerations as more extensive than mere compliance with and adherence to the law.

- TDC Group complies with both Danish and EU rules for privacy and data protection. These rules constitute a minimum and necessary, but not a sufficient, basis for TDC's work with data ethics.
- Rules and regulation often lag behind the rapid pace of technological innovation. Therefore, TDC seeks a proactive approach to data ethics, which is more extensive than legal compliance.

3. TDC seeks to develop a 'positive error culture' among employees, where openness about errors and problems leads to improvement.

- Challenges and dilemmas will necessarily arise, in relation to handling and processing of personal data in a data-extensive environment such as a telecom company. We must be able to discuss and resolve these issues across employee groups and develop a "positive error culture", where errors and problems lead to continuous improvement.
- The precondition for such a culture is that employees feel comfortable coming forward, making public or admitting mistakes, or pointing out areas for potential improvement.

4. TDC prioritizes openness and transparency around the on-going challenges presented by personal data and privacy, in order for companies, organizations and authorities can learn from each other's experiences.

- TDC strives for flawless handling of personal data, but even with the best standards and procedures, errors and data breaches will sometimes occur, either internally or from subcontractors.
- We must learn from our mistakes. Improvement will only occur when we talk openly about them, inform customers, management and authorities, and communicate publicly about the challenges we face.
- TDC has established a whistleblower hotline, to ensure that TDC's employees can draw attention to any perceived legal or internal procedure violations. The hotline can be used in cases where employees believe that others have used system access to obtain information about customers, without a proper work-related need. The hotline can be used anonymously and ensures confidential access to TDC's audit committee and the chairman of TDC's board.
- TDC's employees must be well-informed about data ethics, data security and proper handling of personal data. TDC has prioritized a high standard for employee knowledge through in-depth education and training programs about GDPR and personal data compliance, which all employees must attend and pass.

- 5. Employees that access personal data have signed a declaration of professional secrecy and a confidentiality clause, as part of their employment contract with TDC and have received e-learning education on proper handling of personal data.**
- As a telecommunications operator, TDC invariably handles ordinary, confidential and sensitive personal data. These data are subject to restrictive internal rules for storage and processing.
 - TDC's employees are subject to professional secrecy in relation to customers' personal data, and sign a confidentiality clause, as part of their employment contract. TDC requires that selected employees, who perform particularly sensitive tasks in relation to customer data, must obtain a security clearance from Danish authorities.
- 6. TDC complies with the Telecom Act's requirement to deliver public directory information, but does not not resell confidential or sensitive personal information.**
- TDC resells non-sensitive and non-confidential personal data, through the sale of the public directory information, including name, address and telephone number, in compliance with the Danish Telecom Act's §31. This information is typically utilized for marketing purposes or for charitable organizations conducting nationwide fundraising drives.
 - All customers can opt-out of the public directory, for instance by being registered as a 'unlisted' number. Unlisted users' personal data will not be publicly available and will not be resold.
- 7. TDC only shares customer data with authorities if stipulated by law or a court decision. Emergency or national security situations constitute exceptions.**
- TDC, like all other telecom operators, is subject to legislation which requires collection and retention of personal data. For instance, customers' ability to challenge or correct their billing statements requires retention of data for a specified period. Authorities' ability to resolve criminal acts in cases where courts grant access to information held by telecommunications companies.
 - TDC requires a court order, a decision by a governmental authority, or an injunction, as a requirement for providing customer data to authorities. Exceptions to this principle include emergency law cases, where TDC will collaborate with authorities in the search for lost or missing individuals, regardless of a warrant being issued, as well as national security situations, where the Center for Cyber Security has a mandate to process data traffic of companies with a particularly socially important nature, for the purpose of protecting Danish society against cyber attacks.
- 8. Machine learning, artificial intelligence and use of algorithms shall be used to support TDC's self-help options, and improve services for TDC's customers.**
- Machine learning and other technologies has already been widely adopted by consumers, companies and authorities. TDC uses these technologies to reduce customer support response times, sorting and distribution of customer inquiries, and customer self-service offerings 24 hours a day.
 - TDC will use these technologies for the benefit of our customers, for example through self-service solutions, reduced case processing time and tailor-made offers. The customer must be sure that

actual decisions made by TDC (e.g. termination of customer relationships), will always be finally approved by a human.

- Danish authorities must be able to, on request, access, review and scrutinize TDC algorithms, to verify that they are not programmed to provide discriminatory or “biased” results.