Customer Data Privacy & Security Policy

Dtac is committed to upholding customer data privacy through strict data management, with all dtac staff required to honor customer data privacy and security. Since 2018, dtac has ensured that its customer data privacy and security standard is in compliance with the European Union’s General Data Protection Regulation (GDPR). With effect from 28 May 2018, GDPR applies to all Thai firms that use EU citizens’ data.

Dtac’s “Privacy Policy 2016” can be accessed on the dtac website: https://www.dtac.co.th/document-upload/Privacy\_notice\_th\_29-06-16.pdf. The main points can be summarized as follows:

- Charging Data Records, both voice and data, are encrypted and stored by relevant staff to prevent unauthorized access to and abuse of customers’ personal data;

- Dtac restricts areas storing customer data, with access granted to only authorized staff, so as to ensure that all documents in the areas are secure and safe;

- Just two staff members have the passcode to access important data;

- Dtac assigns selected staff to specifically handle personal data and provides assurances that customer data is processed in line with its Privacy Policy and applicable laws;

- Dtac implements proper technical and organizational management measures to uphold data privacy and security by preventing unauthorized persons from accessing, storing, using, copying, changing or deleting customers’ personal data. In addition, dtac assigns a specialized security team to conduct regular checks on safety measures at its call centers. Staff not allowed to carry on them any kind of flash drives or mobile phones during work hours.

- Dtac may use customers’ personal data for its service development so as to cater its services to serve the different needs of each target group, deliver increasingly better customer experiences, and create innovative services.

- Dtac, with customers’ prior consent, may share or disclose customers’ personal data with/to its subsidiaries for processing that is needed for expanding the scope of services;

- Dtac may disclose customer data when necessary for the purposes of protecting customers and ending any harm against them pursuant to a court order or a legal stipulation that requires personal data to be disclosed to government agencies or government officials;

- Dtac takes steps to ensure that its staff are aware of and understand policies/guidelines on data privacy and security in recognition of the fact that staff have the highest chance to access customers’ personal data. All staff are required to sign an agreement on the protection of customers’ personal data as mentioned in dtac’s Code of Conduct. At dtac, only specific staff are authorized and granted access to customers’ personal data. Random checks are conducted to determine if any staff have accessed or are accessing customers’ personal data without authorization. In the event that unauthorized access is detected, dtac shall immediately suspend the said access and launch an investigation.

In 2018, dtac organized training on the protection of customers’ personal data for its 479 staff members whose work may risk violating the “Privacy Policy 2016”. In addition, internal communications were carried out to promote protection. Assessments were also conducted to check the awareness of data protection among staff with authorized access to customers’ personal data. Checks have not detected any action that may threaten data privacy.