Anti-Money Laundering and Economic Sanctions

To protect Unilever's reputation and avoid criminal liability, it is important not to become associated – however innocently – with the criminal activities of others. In particular, employees must ensure Unilever is in compliance with economic sanctions laws and regulations and does not deal with the proceeds of criminal activities, as this can amount to the criminal offence of money laundering.

This Code Policy sets out essential steps employees must take to avoid breaching economic sanctions rules or being implicated in money laundering.

Musts

Employees **must:**

- Comply with the Responsible Sourcing and Business Partnering Code Policy, the Global Economic Sanctions Global Standard, and any local anti-money laundering or sanctions procedures, when they onboard, contract or monitor third parties
- Immediately notify their Cluster General Counsel if they have any suspicions about actual or potential money laundering activity or about transactions with sanctioned countries or sanctioned third parties
- Obtain prior clearance from their Geography Head, in consultation with their most senior Legal and Finance business partners before allowing any of the following events to happen:

Third party requests to:

- Pay funds to a bank account in the name of a different third party or outside the country of their operation
- Take payments in a form outside the normal terms of business
- Split payments to several bank accounts
- Overpay

Third party payments to Unilever:

- From multiple bank accounts
- From bank accounts from a different geography than the one where the third party is resident
- Deposited in cash when normally made by cheque or electronically
- Received from other third parties that have not been onboarded and/or are not part of the contract
- Made in advance when not part of normal terms of business

Employees involved in engaging or contracting with third parties such as new suppliers, customers and distributors **must**:

- Ensure that the third parties in question are subject to screening to assess their identity and legitimacy before contracts are signed or transactions occur. Various factors will determine the appropriate forms and levels of screening
- Determine, with guidance from their Business Integrity Officer, which tools and processes should be used to facilitate appropriate screening and record-keeping (see the Responsible Sourcing and Business Partnering Policy)
- Carefully consider, where necessary in consultation with their Business Integrity Officer or General Counsel, screening outcomes before deciding whether to do business with the third party

Finance managers who support Supply Chain Management and Customer Development must regularly monitor and / or review suppliers, customers and other third-party service providers to identify business activity or governance that could indicate money laundering is taking place

Must nots

Employees **must not:**

- Simply assume relevant third-party screening has already taken place: failure to check or update screenings periodically may put Unilever and its employees at risk
- Inform a third party suspected of money laundering that they are subject of an internal or external investigation. Employees must obtain guidance from their Cluster General Counsel on how to handle the matter with the third party