

TOOL 1 - CHECKLIST FOR SELF-ASSESSMENT OF PRIVACY/DATA PROTECTION

The “Law, Human Rights and Ethics Checklist for Technology-enabled Community Policing” is a tool designed to help law enforcement agencies intending to use (or already using) technologies, such as mobile device apps and related systems, in community policing to ensure that their activities:

- have bases in law,
- adhere to ethics standards,
- respect human rights law, and
- can help in proving the guilt or innocence of an accused.

LAW AND HUMAN RIGHTS REQUIREMENTS	YES	NO	N/A	COMMENT
LEGALITY				
Does the community policing program have bases in the law or policy of the regulatory framework of policing?				
PRIVACY AND PERSONAL DATA PROTECTION				
Does the community policing program involve processing of personal data?				
Does the community policing program processing of personal data is based in data protection law?				
Does the community policing program process the personal data for explicit, legitimate and specific purposes?				
Does the community policing program process only the minimum data that is necessary for the explicit, legitimate and specific purposes?				
Does the community policing program ensure the personal data is accurate and up to date?				
Does the community policing program retain the personal data for the minimum				

time necessary for the explicit, legitimate and specific purposes?				
Does the community policing program adopt technical and organization measures to ensure that the personal data are secure against unauthorized or unlawful access or disclosure, destruction, alteration, or loss?				
Does the community policing program have a clear, precise and accessible privacy policy that satisfies the requirements of transparency under data protection law?				
Does the community policing program enable data subjects to exercise their rights, such as the right to correct personal data?				
Does the community policing program have a privacy impact assessment and a DPO, following consultation with the privacy authority?				
Does the community policing program comply with the privacy by design principle?				
PRESUMPTION OF INNOCENCE				
Does the community policing program involve in any collection, transmission or storage of material that may be relied upon as evidence?				
Does the community policing program adopt technical and organization measures to protect the probative value of the records it collects, stores or transmits?				
REPUTATION				
Does the community policing program adopt technical and organizational measures to deter its misuse in prejudice to individuals' reputation?				

Does the legal system of the jurisdiction of the law enforcement agency include rules that deter, punish and/or compensate for defamation or malicious prosecution?				
EQUALITY AND NON-DISCRIMINATION				
Does the community policing program adopt technical and organization measures to ensure that it does not discrimination on any of the grounds recognized in human rights law?				
ETHICS				
Does the community policing program adopt any measures that ensure its operations are based on good faith?				
Does the community policing program take any steps to increase its personnel professionalism and capacity?				
Does the community policing program take measures to ensure that its operations are not harmful?				
Does the community policing program any use of force/violence?				
Does the community policing program take measures to ensure confidentiality when the circumstances require so?				
Does the community policing program take measures to ensure that its operations are transparent?				
Does the community policing program establish accountability measures?				
Does the community policing program target generating any financial gain?				