CC4DR RECOMMENDATIONS:
SAFEGUARD DIGITAL RIGHTS WHEN USING COVID-19 RELATED TECHNOLOGIES

As UN Secretary-General António Guterres said recently, the post-COVID19 world will be more digital than before. Human rights are key to shaping the pandemic response, in terms of the public health emergency and the broader impact on people's lives and livelihoods. Human rights put people at the center during this crisis. Therefore, while acknowledging the critical role that digital technologies can play in containing and resolving the current crisis, their application should grant significant consideration of people's digital rights.

We, the Cities Coalition for Digital Rights, with membership of over 50 cities worldwide, have made a commitment towards humane technology, which means considering technologies at the service of people and the public good. Based on our five digital rights principles, we issue the following statement regarding digital rights in relation to COVID-19 related digital technologies, such as contact-tracing applications, video conferencing and learning platforms, geographic mapping, and the use of surveillance tools:

1. Digital tools that are applied to solve the pandemic crisis and to help transition to a 'new normalcy' should not be seen as stand-alone solutions, but rather as **supplements to a comprehensive approach** that includes traditional testing, physical distancing, manual contact tracing, and clinical research. We believe that any use of such technologies (e.g. contact-tracing apps), should not put the fundamental rights of people at risk, and should be accompanied by the implementation of the corresponding epidemiological control measures by the health authorities (availability of protective equipment, tests for detection, manual contact tracing, etc.), and the establishment of new guidelines for social behavior.

2. While considering the possible role of digital technologies in the transition from pandemic phases of containment, mitigation, and rebuilding, we emphasize the need to **respect the rights of citizens**, including **anonymity, transparency, and control** regarding both the medium used and the data collected. The evaluation metrics for the effectiveness of these tools should be clearly determined upfront, and the tools should be monitored once deployed. If their supposed benefit ceases to exceed the cost or risk, they should be deprecated and removed.

3. Those mandated to deploy technologies for crisis response should **avoid fueling asymmetries and inequality.** Digital technologies can have **asymmetrical** impacts, reproducing inequalities existing in the offline world along the lines of income, gender, race and even location. Local and regional governments are the first responders to the COVID-19 crisis and play an essential role in guaranteeing rights protection via local public service provisions, including the most vulnerable populations. Private companies providing technology platforms (e.g. smartphone operating systems) should prevent any unfair impact and not take *any* economic advantage of users when developing apps for pandemic response or recovery.

4. Civil society should be prominently involved in the specification, design, development, and testing of these technologies, with more transparency and openness, including pre- and post-assessment of these technologies. Collaboration with civil society and interaction with local communities will support the democratic, inclusive, and transparent implementation of these technologies, reinforcing democratic control, social cohesion, and leveraging our local societies' knowledge and experience.

5. Our cities should **work together to promote social dialogue on COVID-19 technologies**, with a holistic government approach and through public debate with residents and stakeholders. Now more than ever, it is important to consider the way that technologies, as co-evolving with our social

structures, impact society. We must do so bearing in mind the legacy of these decisions, because setting these norms will likely have long-lasting effects well into the future.

6. Human rights and public health responses go hand-in-hand. A rights-based approach to the design and use of technology to respond to COVID-19 is fundamental to the success of public health response. We believe that if these solutions are implemented, it is essential that the entity that authorizes the use of digital technology solutions, should be the closest possible health authority to citizens, close to and responsive to citizens, while including expertise beyond public health experts in the decision-making process.

Digital technologies, when leveraged in response to the pandemic crisis should follow the Coalition's core principles, which have been integrated into the 10 following principles for this purpose:

1. **Principle of Purpose and Proportionality**. Purpose limitations must be in place. Neither the technologies nor the data collected may be used for purposes other than those deemed strictly necessary for crisis response or recovery.

2. **Principle of Impermanence**. The use of these technologies and data should be limited in time and deleted when no longer needed. Once the risk of pandemic has decreased sufficiently, their use must be reconsidered, and all personal data should be deleted. There should be both technical and legal sunset clauses in place.

3. **Principle of Consent and Trust**. The use of technologies should be voluntary and adhere to notice and consent. They cannot be imposed under any kind of coercion or reward system. Only then can a mutual trust arise.

4. **Principle of Privacy by Design**. The technologies must respect the privacy of users and of all related persons (e.g. contacts). Privacy should be evaluated in the context of the real risks of re-identification or other privacy loss, especially when using highly sensitive information such as healthcare data.

5. **Principle of Control**. Citizens must be considered the primary owners of data they generate through the use of applications and services, where possible. Where applicable, technologies should empower citizens to be stewards of their own data.

6. **Principle of Openness and Transparency**. Technologies should, whenever possible, be developed using open technologies, data models, formats and code, so that the code can be audited, verified, and adopted by other cities and organizations, fostering transparency.

7. **Principle of Responsiveness.** Technologies for COVID-19 should not be stand-alone measures but should draw upon the existing expertise, needs, and requirements of public health authorities and society, culture, and behavior, if they are to be effective in combatting the pandemic.

8. **Principle of Participation.** The development of such technologies should consider the needs of all people and include strong feedback loops between policymakers and citizens, with opportunities for iteration. Human rights should be explicitly taken into account in the selection of solution providers and in the process of technical development.

9. **Principle of Social Innovation.** The successful and equitable use of these technologies requires a focus on social innovation, not merely on technological innovation

when they are to be used in everyday life in our societies. Collective social intelligence, behavior, and social cohesion are equally important.

10. **Principle of Fairness and Inclusion.** Technologies must be accessible and serve all people, assuring equal access and equal treatment across communities. Technologies should be used to eliminate social inequalities while paying particular attention to marginalized groups.

<div align="center">================================</div>

BACKGROUND STATEMENT:
CC4DR VIEW ON COVID-19 RELATED TECHNOLOGIES

We stress that human rights, privacy, and public health responses go hand-in-hand. A rights-based approach to the design and use of technology to respond to the pandemic crisis is fundamental to the success of public health responses during and after containment. Public health initiatives rely on public buy-in and participation, which in turn rely on public trust. Public trust is reinforced when the public sees that their right to privacy and human rights principles such as transparency and non-discrimination are respected. The Cities Coalition for Digital Rights has made a commitment towards humane technology, which means perceiving technologies in a broader social context by putting them at the service of the people and the public good. While digital technologies offer many possibilities, we need to consider the conditions for their use and democratize this process. Now more than ever it is important to see technology as social structures, serving communities and society as a whole. We must do so bearing in mind the legacy of these decisions, as setting these norms will have long-lasting effects into the future with unforeseen social consequences.

Governments are promoting or implementing different technologies to provide insights into general health, to contain virus spread, and to assist epidemiological services related to COVID-19. These include apps that inform, map, offer self-diagnosis, track symptoms, or trace contacts. These technologies can clearly impact citizens' rights. Apart from the impact on privacy regarding the protection of personal data and the expectation of anonymity in sensitive areas like healthcare, these technologies can also impact physical and psychological well-being, identity, and autonomy. They can limit or jeopardize freedom of association, the right to security, the right to health, the right to work, and the right to non-discrimination. Additionally, digital surveillance can introduce various types of risk, such as limiting the agency of individuals or communities by monitoring behavior or by mapping and categorizing communities in potentially harmful ways.

BACKGROUND ON PRINCIPLES FOR COVID-19 RELATED DIGITAL TECHNOLOGIES

- Purpose and time limitations

The technologies deployed and the data collected should be used only for the purposes necessary to manage the crisis and should be the minimum necessary to do so. The technologies should not be used to collect other data for other uses or to use the data in additional ways. These purposes should be clearly communicated to citizens.

For example, contact tracing applications should only be permitted for two specific purposes in the context of the outbreak: 1) to help break chains of transmission, or 2) to help track the spread of the virus in order to assess or implement other response measures.

Depending on their design, these apps can record information about contacts that a person has throughout the day. The data should then be used solely for contact tracing

and the use of the data and the technology should be limited in time. Once the risk of pandemic has decreased sufficiently, the technologies should no longer be used. After the temporary use of an application, a user should be able to deactivate or uninstall the app from all devices, and delete their user data.

These technologies must be properly developed in order to provide accurate, effective and useful results, minimizing false positives or negatives. The way false positives and false negatives can vary by subcommunity should also be considered and evaluated; performance that may be acceptable for the general population as a whole can mask unacceptable performance for a minority or subset of it.

We should also consider the risks even when the apps work seemingly as intended (true positives and true negatives). These applications *may* support the possibility of greater freedom of movement but may also contribute to a false sense of security. The effectiveness of these apps has not been yet proven, both due to experiences in the first examples of use, as well as because of the number of users required to ensure accuracy or added value of the app (which has been estimated to be 60% of the population or more). For example, the largest source of false negatives is likely to be from those who are not using the contact tracing app in the first place.

Finally, such apps should be understood as one tool among many to help authorities contain the spread and possibly identify sources of infection. A technology such as contact-tracing applications can't be a stand-alone measure against COVID-19 but has to work hand-in-hand with medical and social measures, such as mass testing, if it is to be effective. Cities must consider where technologies are of added-value for data-driven decision making and where human judgment is called for. Technologies are rarely the solution to these kinds of problems.

- Data protection and control over personal data

The use of technologies should be voluntary, in the same way as the adoption of any technology for personal use and cannot be imposed under any kind of coercion. No one should be discriminated against for not using an application at the request of government. These tools should not be mandatory nor penalize citizens for choosing not to use them. Moreover, while using such apps, citizens should have control over their data and options for data portability when possible.

Especially in the case of contact tracing apps, technologies must be designed, developed, and deployed based on current best practices in privacy engineering and cybersecurity in order to minimize the occurrence of any data leaks, data de-anonymization, and other partial losses of privacy. The technologies must respect the privacy of users and their contacts. Communications should be encrypted in such a way that if they are intercepted it should not be possible to deduce the fact that an individual is infected. A chain of contacts should not be interpretable out of context, and it should also not be possible to interrelate one person's contacts with another's. COVID-19 technologies should comply with current legislation on data protection and confidentiality of electronic communications. Such legislation can vary by jurisdiction but includes the General Data Protection Regulation (GDPR) in Europe and the Health Insurance Portability and Accountability Act (HIPAA) in the United States.

These technologies must be evaluated to ensure they provide accurate, effective, and useful results. Proper measures, including giving citizens the option for human interaction with health authorities, must be implemented in order to avoid panic, lack of information, or doubts based on an application's notifications.

- Eliminate asymmetrical effects across communities

Local and regional governments need to have the means in order to ensure that digitalization does not exacerbate inequalities and serves to bridge the existing socioeconomic divide. Technology will be vital in the protection of local democratic principles and in ensuring equitable citizen participation and open and inclusive decision-making processes. Communities must be at the forefront of shaping the technology of the future in order to maintain sustainable ways of life. Technologies must serve people, and work towards reducing or eliminating social inequalities, paying particular attention to marginalized groups, including minorities, women and girls, children and youth, older persons, persons with disabilities, and poor households. The concept of "marginalized group" should also be considered broadly and not be limited to demographic or socioeconomic attributes; individuals can also be disadvantaged by lack of access to resources such as the internet or parks, or they may not speak the primary language.

These technologies must aim to serve the public good via communities, to reinforce social cohesion, equal access, and leverage social intelligence. Local authorities need to think broadly about how these technologies can be most inclusive and accessible, ranging from high-tech to simpler, low-tech solutions, and facilitate communication in all directions. In order to avoid worsening the digital divide, local governments need to adequately implement technologies and other measures, such as non-digital surveys or outreach to community leaders, that help them understand the gaps and needs relating to COVID-19 related situations of all members of their communities.

- Defining societal norms together

While digital technologies offer many possibilities, we need to consider the conditions for their use and democratize this process. Awareness has increased recently on how technology affects the human rights of both individuals and groups, which must be protected online and offline, so that citizens are safe in both real and virtual worlds, in public and in private spaces.

Technologies dealing with societal issues such as COVID-19 and deconfinement require a strong feedback loop between policymakers and citizens. Collaboration and collective intelligence are key in defining how these technologies can be adapted and optimized for the current situation. Indicators for success will need expertise beyond technical, governmental, and epidemiological views on welfare.

The successful use of these technologies requires social innovation as much as technological innovation when they are to be used in everyday life in our societies. Their deployment should be accompanied by an awareness that these collective choices are defining (new) societal processes and norms in the long run.

Technologies should always be developed according to the principles of transparency and openness. When practical, technologies should be developed in open source formats and technologies, and decentralized architectures are preferred over centralized ones, all else

being equal. Published source code: a) can be audited and verified, and b) can be adopted by other cities and entities. However, transparency need not be, and should not be, viewed as synonymous with open source, which is not always possible. Technologies can be accompanied with design and architecture details explaining how they work and what concrete steps were taken to mitigate various risks, even if it is infeasible for the source code itself to be open. Reference implementations can also be provided. The inability to publish full source code should not be viewed as a license to avoid other means of providing transparency.

Similarly, there must be digital rights-based accountability criteria regarding the selection of the technologies' provider, and technology design and choice. This enables promoters of the technologies to show how they work, and why and how decisions are made based on the insights generated by the technology and data. Criteria of human rights should be explicitly used in the selection of solution providers and technical development, and the technologies on which they are based.

Private vendors should not take advantage when technology is developed or deployed for the purpose of combatting this pandemic. This includes, for example, not requiring individuals to sign up for or participate in their existing commercial offerings in order to use pandemic-related services. The contributions of private companies should not prevent the deployment of official governmental solutions, or other competing solutions, on private platforms.

The Cities Coalition for Digital Rights presents this statement and the associated principles to protect human rights and preserve public trust. Governments, civil society organizations, and the private sector can work together to ensure that digital technologies are used responsibly during the COVID-19 crisis. If done correctly and with digital rights in mind, we will have a stronger understanding of and proven best practices for leveraging such technologies during public health crises.

We stress that this document puts forward recommendations to specifically safeguard digital rights in cities, when using pandemic related digital technologies. We acknowledge that local authorities, simultaneously, have the responsibility to safeguard health, safety, and freedom of movement.

We take into account that different cities have different legislative contexts nationally and regionally. This set of recommendations can be adjusted according to local needs.

[END OF STATEMENT]