EN

ANNEX 8

Of the Commission Implementing Decision on the 2020 Annual Action programme for the Partnership Instrument

**Action Document for International Digital Cooperation - Personal data protection and data flows**

## 1 Key identification data

<table>
<thead>
<tr>
<th>Title of the Action</th>
<th>International Digital Cooperation - Personal data protection and data flows</th>
</tr>
</thead>
<tbody>
<tr>
<td>Country/region/global</td>
<td>Global: Asia, Africa and Latin America</td>
</tr>
<tr>
<td>Sector of intervention</td>
<td>International digital cooperation</td>
</tr>
</tbody>
</table>
| Indicative budget | Total: 3 000 000 EUR  
EC contribution: 3 000 000 EUR  
Other contributions: N/A |
| Duration and target start date of implementation | Duration: 42 months  
Target start date: mid 2020 |
| Method of implementation | Direct management - Procurement |
| DAC code(s) | 99810 |

### Markers

<table>
<thead>
<tr>
<th>General policy objective</th>
<th>Not targeted</th>
<th>Significant objective</th>
<th>Principal objective</th>
</tr>
</thead>
<tbody>
<tr>
<td>Participation development/good governance</td>
<td>X</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>Aid to environment</td>
<td>X</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>Gender equality</td>
<td>X</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>Trade Development</td>
<td>X</td>
<td>☐</td>
<td>☐</td>
</tr>
</tbody>
</table>

**RIO Convention markers**

| Biological diversity | X | ☐ | ☐ |
| Combat desertification | X | ☐ | ☐ |
| Climate change mitigation | X | ☐ | ☐ |
| Climate change adaptation | X | ☐ | ☐ |
2 RATIONALE AND CONTEXT

The General Data Protection Regulation (GDPR) applies across the European Union since more than one year. It is at the centre of a coherent and modernised EU data protection regime that also includes the Data Protection Law Enforcement Directive and the Data Protection Regulation for EU institutions and bodies. The EU legislative framework on data protection is a cornerstone of the Digital Single Market and the European human-centric approach to innovation. It is becoming part of the regulatory floor for a widening range of policies including health and research, artificial intelligence, transport, energy, competition and law enforcement.

Strong data protection rules are essential to guarantee the rights of individuals, but also for the functioning of democratic societies as a whole. Moreover, as a trust enabler, data protection has become a key component of the digital economy as well as regulatory and law enforcement cooperation between public authorities.

This is increasingly recognised at global level and many countries have adopted or are in the process of adopting modern and comprehensive data protection rules based on principles similar to those of the Regulation. This offers new opportunities to facilitate cross-border data flows, between commercial operators or public authorities, while improving the level of protection for individuals across the globe.

2.1 Action summary

The EU aspires to be a world leader in the digital economy to seize the many opportunities that the digital transformation offers. Data flows, including the exchange of personal data, are an essential element of the digital economy, and are particularly important for the EU as the world’s first exporter of digital services. The EU therefore has a strong interest in facilitating such data flows, on which not only trade but also cooperation between public authorities in different fields (e.g. law enforcement) increasingly rely. At the same time, the protection of personal data is a fundamental right in the EU, which therefore has to ensure that data transfers to third countries do not undermine the guarantees afforded within the EU.

The best way to achieve these objectives is to work towards convergence of the data protection frameworks of third countries with that of the EU. Such (upward) convergence also opens the way for so-called adequacy findings that within the EU’s “toolbox” for data transfers constitute the most comprehensive instrument as they essentially treat the third country, for the purpose of data protection, as part of the EU internal market. In its 2017 Communication on “Exchanging and Protecting Personal Data in a Globalised World”¹, the Commission recognized the importance of this instrument in pursuing the EU’s strategic objectives with respect to both data flows and data protection. As such, the action projects externally the Commission priority 2019-2024: A Europe fit for the Digital Age. Building on the very positive results of the first phase and considering the further increase in importance of data protection policy in international trade and regulatory cooperation across borders, the proposed action intends to pursue the following outcomes:

- Increase awareness of the importance of personal data protection as a pre-requisite to data exchanges with the EU;
- Enhance the knowledge of the EU data protection legal framework in partner countries;
- Encourage international convergence towards the EU model of data protection;
- Develop common approaches to personal data protection, involving public authorities, private sector, academia and civil society organisations.

Ultimately, by promoting convergence with the EU standards, the action will contribute to creating a level playing field for EU companies worldwide.

¹ COM/2017/07 final.
2.2 Background/Context/Rationale for PI funding

The demand for protection of personal data is not limited to the EU. A growing number of companies are addressing these concerns by extending of their own volition the rights created by the GDPR to their non-EU based customers. Moreover, as countries around the world are increasingly addressing similar challenges, they are equipping themselves with new data protection rules or modernising existing ones. These laws often have a number of common features that are shared by the EU data protection regime, such as an overarching legislation rather than sectorial rules, core data protection principles, enforceable individual rights and an independent supervisory authority.

This trend is truly global, covering countries from South Korea to Brazil, from Chile to Thailand, and from India to Indonesia. The increasingly universal membership of the Council of Europe’s ‘Convention 108’ – recently modernised\(^2\) – is another clear sign of this trend of upward convergence.

Promoting safe and free data flows through adequacy decisions and beyond

This developing convergence offers new opportunities to facilitate data flows, and consequently trade, as well as cooperation between public authorities, while improving the level of protection for the data of individuals in the EU when it is transferred abroad. Implementing the strategy laid out in its 2017 Communication on “Exchanging and Protecting Personal Data in a Globalised World”, the Commission intensified its engagement with third countries and other international partners, building on and further developing elements of convergence between privacy systems. This included exploring the possibility of adopting adequacy findings with selected third countries. This work has yielded important results, in particular the entry into force in February 2019 of the EU-Japan mutual adequacy arrangement that created the world’s largest area of free and safe data flows.

Adequacy discussions with South Korea are at an advanced stage and exploratory work is ongoing with a view to launching adequacy talks with several Latin American countries – such as Chile, Brazil and Colombia – depending on the completion of ongoing legislative processes. Developments are also promising in some parts of Asia, such as India, Indonesia, Taiwan and Thailand, as well as in the European Eastern and Southern neighbourhood, which could open the door to future adequacy decisions.

Moreover, a number of countries have put in place transfer instruments similar to the GDPR’s adequacy decision, and on that basis have recognised both the EU and third countries recognised by the EU as ‘adequate’ as safe havens for data transfers. This has the potential to create a network of countries where data can flow freely.

Beyond working on bilateral tools, there is an increasing interest at global level to cooperate on data protection. For instance, Japan has launched a series of initiatives (the “Data Free Flow with Trust” initiative and the “Data Security Alliance”) that aim to bring together like-minded partners to facilitate data flows among them while protecting data against undue interference from governments of countries that do not share our values.

Developing new synergies between trade and data protection instruments

While promoting convergence of data protection standards at international level, the Commission is also determined to tackle digital protectionism. To that end, it has developed specific provisions on data flows and data protection in trade agreements which it systematically tables in its bilateral and multilateral negotiations, such as the current WTO e-commerce talks. These horizontal provisions rule out purely protectionist measures, such as forced data localisation requirements, while preserving the regulatory autonomy of the parties to protect the fundamental right to data protection.

Whereas dialogues on data protection and trade negotiations must follow separate tracks, they can complement each other: the EU-Japan mutual adequacy arrangement is the best example of such synergies, further easing commercial exchanges and in this way amplifying the benefits of the

\(^2\) Convention 108+, as agreed in the 128th Session of the Committee of Ministers at Elsinore, Denmark, 17-18 May 2018.
Economic Partnership Agreement. In fact, this type of convergence, based on shared values and high standards and backed-up by effective enforcement, provides the strongest foundation for the exchange of personal data, something which is increasingly recognised by our international partners.

Given that companies increasingly operate across borders and prefer to apply similar sets of rules in all their business operations worldwide, such convergence helps to create an environment conducive to direct investment, facilitating trade and improving trust between commercial partners.

Facilitating the exchange of information to combat crime and terrorism based on appropriate safeguards

Greater compatibility between data protection regimes can also significantly facilitate the much needed exchange of information between EU and foreign regulatory, police and judicial authorities and, in this way, contribute to more effective and rapid law enforcement cooperation. To that end, the Commission has the possibility to adopt adequacy decisions or international agreements providing appropriate data protection safeguards under the Law Enforcement Directive to deepen its cooperation with key partners in the fight against crime and terrorism. Examples demonstrating the importance of high data protection standards as a basis for stable law enforcement cooperation with third countries are the transfer of Passenger Name Records (PNR), or the exchange of operational information between Europol and competent law enforcement authorities of a third country or international organisations. In this regard, negotiations on international agreements are currently ongoing or in preparation with several countries of the Southern Neighbourhood, as well as with Turkey and New Zealand.

Increased compatibility between data protection regimes can also play an important role in the multilateral context, in particular concerning initiatives to combat cybercrime or financial crime. As an example, the current negotiation of a Second Additional Protocol to the Budapest Convention shows the need of having a common set of shared principles and rules to allow for effective cooperation between law enforcement authorities. Another example is the interest expressed by Ameripol (a police cooperation organisation for the Americas) to cooperate with the Commission in the development of data protection standards.

Promoting cooperation between data protection enforcers

At a time when data protection compliance issues or security incidents may affect large numbers of individuals simultaneously in several jurisdictions, closer forms of cooperation between supervisory authorities at international level can help ensure both a more effective protection of individual rights and a more stable environment for business operators. Against that background, and in close contact with the European Data Protection Board, the Commission has committed to work on ways to facilitate enforcement cooperation and mutual assistance between EU and foreign supervisory authorities.

Finally, the Commission also has committed to step up its dialogue with regional organisations and networks, such as the Association of Southeast Asian Nations (ASEAN), the Asia Pacific Privacy Authorities forum (APPA), the African Union (AU) or the Ibero-American Data Protection Network, which play an increasingly important role in shaping common data protection standards, including on cross-border data exchanges, promoting the exchange of best practices and fostering cooperation between enforcers. For instance, representatives of ASEAN have suggested to enter into a closer dialogue and ‘compare notes’ on the development of transfers tools such as model contract clauses or certification schemes. The Commission also works with the Organization for Economic Cooperation and Development (OECD) and the Asian-Pacific Economic Cooperation Organisation (APEC) to build convergence towards a high level of data protection.

2.3 Lessons learnt

As reflected, for instance, in the reference to the concept of ‘Data Free Flow with Trust’ in the Osaka G20 Leaders’ Declaration: https://www.consilium.europa.eu/media/40124/final_g20_osaka_leaders_declaration.pdf
The proposed project builds on the current PI-financed project, which has already produced excellent results, influencing numerous policy and legislative processes in the current focus regions through close interactions with key decision-makers and stakeholders. This includes developments at both regional level (e.g. the drafting of the Ibero-American Data Protection Standards⁴) and country level (e.g. the adoption of data protection legislation in line with EU standards in Brazil).

For instance, activities (engagement with policy-makers, conferences, media publications, DPO training course, etc.) carried out in Brazil, Chile and Argentina as regards Latin America, or in India, Thailand and Indonesia as regards Asia have demonstrated the potential of this type of actions based on a strategic presence enabled through the collaboration with local experts.

At the same time, the experience gained from these activities also shows the need to continue our efforts and intensify our contacts with the government and other stakeholders in these regions. For example, in Latin America, Ecuador just tabled the first ever bill in this area in October 2019, while Chile and Paraguay are debating draft laws. Similar initiatives have also been taken in many countries of Central America and the Caribbean, from Panama to Barbados or Jamaica. In Asia, countries like Sri Lanka and Thailand recently adopted data protection laws, while others like India and Indonesia are in the process of doing so. The Commission can play an important role in these processes by providing technical know-how, explaining the benefits of strong data protection rules and thus helping to overcome opposition. Even where new data protection laws have already been enacted, there is often the need for further implementation work, in particular the setting up of the data protection authority, to render the law effective. This offers further opportunities for collaboration, for instance by providing technical know-how and support to the newly created DPA, build up enforcement cooperation with other supervisory authorities, assist in the development of guidelines, etc.

At regional level, the Commission has established close contacts with the Ibero-American Network of Data Protection Authorities and has been asked to provide input into the development of data protection standards by Ameripol (the Latin American equivalent of Europol). Also, the Organization of American States has just launched an important initiative towards the modernization of its own data protection principles taking as a reference the Ibero-American Data Protection Standards. Another example for future collaboration is ASEAN, which has expressed its interest in a dialogue with the Commission on the development of data transfers instruments such as Standard Contractual Clauses. With many governments and other stakeholders looking towards the EU and its new data protection framework for inspiration, all of these initiatives offer considerable opportunities to promote upward convergence.

As data protection regimes become an increasingly global phenomenon, there is a strong argument for further extending the project to other strategic target areas, in particular Africa, which is rapidly “digitizing” and where important developments in data protection are taking place. This concerns again both the regional level – with the development of the African Union Convention on Cyber Security and Personal Data Protection, the activities of the Association of Francophone Data Protection Authorities as well as the establishment of pan-African forums such as the Africa Region Data Protection and Privacy Conference (AFRICA-DPPC) or the Data Protection Africa Summit – and in individual countries (e.g. Kenya, Senegal, Togo, Nigeria, Rwanda, Morocco, Ghana or Tunisia), several of which have also joined the Council of Europe data protection Convention 108⁵. While Africa is the most underdeveloped region with respect to data protection – fewer than 10 out of 53 African nations have comprehensive data protection laws – there is clearly a momentum and increasing efforts to cooperate across Africa and with other partners, in particular the EU. With the EU, this should be seen in the broader context of the New Africa-Europe Digital Economy Partnership, which has as one of its central objectives to provide support to the development of an African Single Digital Market.

---

⁴ Since their adoption in 2017, the Ibero-American Data Protection Standards have played an important role as a blueprint for privacy laws in the region and as a platform for closer cooperation between data protection authorities.

⁵ The Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (convention 108) is the first international data protection legally binding instrument, which is open for signature to countries that are not members of that organisation. Currently, Cabo Verde, Mauritius, Morocco, Senegal and Tunisia are Parties, while Gabon and Ghana are Observers.
As regards the EU, harmonised data protection rules across Africa form a central element of such a single market. There is therefore a great potential for promoting the EU’s values, foster dialogue with African partners and influence the development of data protection laws across the continent via this Action.

Extending the project to this region would also be in line with the objectives of the new ‘Africa - Europe Alliance for Sustainable Investment and Jobs’ (launched in September 2018) which aims to take the EU’s partnership with Africa to the next level by deepening economic relations and boosting trade, with data protection as a precondition for facilitating data flows. In this regard, the project should support engagement with relevant stakeholders at regional level, including the Smart Africa Alliance and the African Union Commission, as well as bilaterally with those countries that are pioneering in developing modern data protection frameworks. In particular, representatives of the African Union have already expressed their interest in closer collaboration with the EU in working towards greater harmonisation of data protection laws in Africa, as a basis for the African digital single market and a complement to the recently concluded Continental FTA. It is also important to consider the role played by the Regional Economic Communities, like ECOWAS (the Economic Community of West African States) or COMESA (the Common Market for Eastern and Southern Africa).

More generally, promoting data protection in developing countries can play an important role in strengthening both the rule of law/democratic governance and the competitiveness of the economy, thereby increasing the attractiveness for foreign investment.

The EU has a particular interest in law enforcement cooperation, including with the North African countries. With a view to strengthen Europol's collaboration with third countries in the fight against terrorism and other serious transnational crime, the Commission has recently received a mandate to negotiate international agreements with eight countries (Algeria, Egypt, Israel, Jordan, Lebanon, Morocco, Tunisia and Turkey) to allow exchanging personal data with Europol. A similar competence has been conferred for cooperation agreements by Eurojust. In addition, the Commission is tasked to review the existing Europol cooperation agreements. In all these cases, the central aspect is to ensure that appropriate data protection safeguards are provided. In many cases, this will require as a first step a strengthening of the domestic data protection regime. The Project can play an important role in this context.

Lastly, as lawmakers from many countries around the world are developing and implementing data protection frameworks, they face common challenges and questions. This also applies to those countries that have recently adopted/updated their framework for data protection and that seek to ensure that the authorities charged with the implementation and enforcement of the law are fully prepared and equipped to carry out their tasks. Countries like Brazil, Thailand and Sri Lanka have expressed a key interest in learning from the EU experience and are looking for support in building capacity. Building on prior experience with the DPO certification for Indonesian government officials that the Project supported, the Commission is collaborating with Maastricht University in setting up a “Data Protection Academy” that could offer hands-on training to both policy-makers and representatives from (in particular newly created) supervisory authorities.

2.4 Coherence and complementarity

The proposed action should be carried out taking into consideration (and, when relevant, ensuring consistency with) at least the following bodies and related initiatives:

- European Data Protection Board
- Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, as modernised (Convention 108+)
- On-going negotiations of the second Additional Protocol to the Council of Europe Convention on Cybercrime (Budapest Convention)
- African Union Convention on Cyber-Security and Personal Data Protection
- OECD Privacy Framework
- ASEAN Working Group on Digital Data Governance
Furthermore, the proposed action will seek complementarities with the project “Cross-border access to electronic evidence - SIRIUS” implemented with Europol and Eurojust under the lead of DG HOME and DG JUST. This project started implementation in 2018. It aims to support enhanced cooperation for law enforcement purposes between the EU and the US through more effective EU-US MLA procedures and strengthened direct cooperation between law enforcement and US-based online service providers for access to digital evidence. A phase II of this project is currently in preparation to expand its geographical scope to include third countries other than the US.

The project team will ensure coordination and analyse possible synergies with other EU funded projects:

1) EU Cyber Direct (PI), with EUISS: supports EU cyber diplomacy efforts and consequently contributes to the development of a secure, stable and rights-based international order in cyberspace through extensive dialogues, in particular with strategic partners from Brazil, China, India, Japan, South Korea, the United States, as well as regions of Latin America and the Asia-Pacific. The project brings together governments and non-governmental actors to explore the main issues surrounding international law in cyberspace, norms of responsible state behaviour and confidence building measures. Workshops, conferences and meetings organized in the framework of EU Cyber Direct contribute to a better understanding of EU cyber diplomacy and cyber resilience policies worldwide.


3) Cyber4D (DEVCO): implemented with the Northern Ireland Cooperation Overseas (NICO), in consortium with UK FCO, Dutch MFA and Estonian RIA, this project is aimed at supporting and further facilitating the development of cyber resilience in partner countries while promoting an inclusive multi-stakeholder and rights-based approach and ensuring compliance with the rule of law and good governance principles. Objectives/components: Increased awareness of decision-makers on cybersecurity and facilitation of adoption and implementation of consistent, holistic and actionable national cybersecurity. Increased local operational capacities to adequately prevent, respond to and address cyber security incidents (Computer Security Incident Response Teams and improved formal and informal cooperation in the national cyber ecosystem). Intensified awareness of associate countries and promotion of cybersecurity good practices globally. Geographical scope: Africa and Asia.

4) EU Cyber Capacity Building Network - CyberNet (DEVCO): implemented with the Estonian Information’s System Authority. Aimed at strengthening global delivery, coordination and coherence of EU’s external cyber projects and the EU’s own capacity to provide TA to third countries in the field of cyber-security. The main expected result is to establish and maintain a network of organisations and a create a pool of experts to be used in cyber capacity building activities in partner countries by providing support to Commission Services, EEAS and EU Delegations. Geographical scope: Global.

2.5 EU added value
As mentioned in Section 2, the EU legislative framework on data protection is a cornerstone of the Digital Single Market and the European human-centric approach to innovation. Through this FPI Action, the EU is able to significantly contribute to increasing awareness, understanding of and support for the key features of a modern data protection regime and which are shared by the EU.

The EU has a strong interest to promote regulatory convergence with our own framework of emerging data protection regimes around the world. Under EU law, one of the instruments recognising the highest level of convergence is an adequacy finding of the Commission, which establishes that a non-EU country provides a level of data protection that is “essentially equivalent” to that of the EU.

No EU Member State has competence, by itself, to assess and determine whether the level of data protection in a third country is essentially equivalent to that of the EU.

At the same time, the EU data protection acquis provides for a wide range of alternative transfer tools, which should also be used to facilitate cooperation between EU supervisory and law enforcement authorities and their international partners.

Therefore this FPI Action will support the Commission in ensuring coherence of the internal and external dimension of EU data protection policy and promote strong data protection at international level to improve law enforcement cooperation, contribute to free trade and develop high personal data protection standards globally.

2.6 Cross-cutting issues

The aim of this project is to support global convergence of personal data protection regimes based on modern and strong protections and supporting international data flows. The protection of personal data is a fundamental right in the EU, which therefore has to ensure that data transfers to third countries do not undermine the guarantees afforded within the EU. Moreover, as strong data protection rules are essential to guarantee the rights of individuals and increasingly to ensure the good functioning of democratic societies as a whole, this objective is directly tied to the following cross-cutting issues: democracy, rule of law, human rights and fundamental freedoms.

3 ACTION DESCRIPTION

In light of the above, the Commission pursues the objective to promote convergence on a global scale and would use this action to focus on Asia, Africa and Latin America.

It is crucial to sustain and broaden the activities that have been developed in the context of phase I of this Project. An extension for three additional years would help to ensure the consolidation of the current results as well as to complement the work carried out so far with new actions targeted both at further actors in Asia/Latin America and (for the first time) in Africa, building on the success of the Project so far.

This objective would be pursued by spreading the knowledge of the EU’s data protection acquis, by supporting partner countries in their efforts to put in place for the first time, or to strengthen existing data protection laws and by cooperating in regional or global initiatives to build convergence, through the development of common standards, the exchange of best practices, etc.

The activities will be tailored per target region/country. One of the key success factors of the current Project has been the work with Regional and National key experts, which are playing a pivotal role in developing its core activities. Given also the increased scope of the future Project, it is thus foreseen to develop a network of experts – including EU relevant data protection experts to allow a proactive and dynamic response and to reply to the ever-increasing demand from different stakeholders.

The Project will also rely on capacity building activities like training programs for new regulators, exchange programs and secondment activities. The idea of creating training programs and study visits for policy-makers and supervisory authorities in third countries has proven successful with an ad-hoc program for representatives of the government of Indonesia. The next phase of the Project will allow
for further consolidation and replication of this kind of actions with more countries, building on the cooperation with the Maastricht University and possibly other academic institutions to develop a Data Protection Academy tailored to third countries’ legislators and data protection authorities.

In addition to the above, the future Project will also reinforce ties with the private sector, both business and civil society, in partner countries.

### 3.1 Objectives

The overall objective of this Action is to continue to contribute to the development of a secure, right-based international digital sphere, conducive to a level playing field in terms of market access and business opportunities for EU companies.

The specific objectives of this action, which will contribute to the achievement of the overall objective, are:

- **SO1.** To promote a common understanding of the importance of personal data protection for cross-border data flows.

- **SO2.** To influence an approach to personal data protection in the partner countries/regions compatible with the EU framework in order to facilitate an international level playing field for businesses, respecting citizens’ rights in the digital age.

To achieve the above objectives, this action will work towards the consolidation or development of the following expected results:

- **R.1.** Increased awareness of relevant actors and in particular public authorities, civil society and business of the importance of personal data protection as a pre-requisite to cross-border data flows with the EU;

- **R.2.** Enhanced knowledge of target groups in partner countries of the EU data protection legal framework;

- **R.3.** Increased international convergence on data protection principles as a way to strengthen compatibility with the EU model of data protection;

- **R.4.** Development of common approaches to personal data protection, involving public authorities, private sector, academia and civil society organisations.

The activities will consist of the elements presented below, the details and exact extent of which will be specified per country/region:

- Research activities and intelligence gathering on data protection developments will be essential to support the specific outreach actions of the Project.

- Furthermore, other activities undertaken in the initial period of the Project will identify best practices/lessons learned on how to implement a modern data protection regime.

- The research/intelligence work will produce reports and briefings and will lead up to the main activity which consists of specialised conferences/workshops, in-country roundtables, outreach (e.g. decision-makers, business associations, NGOs) and participation in already planned events.

- Trainings and study visits for policy-makers and data protection authorities.

- Communication and information dissemination activities to promote our key messages (mainly via the new website developed as part of the current Project, social media and printed material).

Meetings will be held for all outcomes (R.1, R.2, R.3, R.4) for the exchange of best practices with relevant stakeholders on selected issues (the final list to be adopted after the research activity). The activities will be specialised in nature and focus on a targeted audience of policy-makers and data protection authorities (e.g. ministries, government authorities, legislators) directly involved with the issue, business, academia and specialised civil society representatives. In general, a multistakeholder approach, involving different categories of stakeholders in the same events will be favoured. The exact format for the respective outcomes will be decided in cooperation with the partners. In countries where a national
data protection authority is in place, the activities may be linked to those of the authority (e.g.,
conferences of regional bodies, etc.) and proposals may be developed for ongoing coordination
activities.

The outcomes of these activities should be disseminated as widely as possible in order to increase
awareness, ensure the optimal sharing of best practices and lessons learned and therefore progressively
contribute to common approaches.

The expected impacts of this action include:

- Progressive convergence of partner countries’ legal frameworks with the EU;
- Reinforced channels of cooperation/dialogue with relevant partner countries, including between
  public authorities.
- Strengthening of regional initiatives, ensuring consistency and promoting convergence with the
  EU data protection legal framework.
- A corpus of updated knowledge on data protection regimes available to all interested partners and
  accessible through digital means.
- A collaborative network of data protection specialists at both regional and global level.

This developing convergence offers new opportunities to facilitate data flows, and consequently trade
as well as cooperation between public authorities, while improving the level of protection for the data
of individuals in the EU when it is transferred abroad.

These impacts are expected to persist beyond the implementation period of the proposed action. Activities
conducted through the proposed action are expected to, and will be further designed with a view to, create positive spill-over effects in the partner countries.

### 3.2 Stakeholders

The Project shall not duplicate the work of existing fora like the International Conference of Data
Protection and Privacy Commissioners (ICDPPC) or the Consultative Committee of the Convention
for the Protection of Individuals with regard to Automatic Processing of Personal Data (T-PD). In all
countries/regions, in addition to civil society, the Project shall target relevant partners which include:

- Relevant national Ministries involved in data protection matters (e.g. of Communication and
  Information Technology, Trade, Economy, Finance) and relevant regulatory authorities (e.g. data
  protection authorities; cybersecurity authorities/agencies)
- Members of national Parliaments and key staffers
- NGOs and business representatives
- Key regional and sub-regional organisations and networks (such as ASEAN, APPA, APEC,
  the African Union, Africa-DPPC, the Ibero-American Data Protection Network, OAS).

### 3.3 Risk assessment and management

There are a number of risks associated with the implementation of the proposed action. They include:

<table>
<thead>
<tr>
<th>Risk description</th>
<th>Risk level (High, Medium, Low)</th>
<th>Mitigating measure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interest of partner countries to participate in Project activities decreases</td>
<td>Low</td>
<td>Action needs to showcase the added value for engagement</td>
</tr>
<tr>
<td>Sufficiently involving all stakeholders and managing the dynamics in the partner countries and at regional level proves challenging.</td>
<td>Medium</td>
<td>Adoption of a balanced intervention approach by way of a mix of actions at national, regional and continental level including clearly defined decision</td>
</tr>
</tbody>
</table>
3.4 Communication and EU visibility

Communication and visibility will continue being an integral part of the action. The project has already elaborated a Communication strategy approved by DG JUST. This strategy guides all communication related activities. As part of this strategy, the project has supported the creation of a website to support the external action of DG JUST in this domain and contribute to the achievement of the objectives of the project. This website was been set up in close collaboration with the Communication Department of DG JUST, DG COMM and DIGIT to ensure the compatibility of the website of the project with the Europa.eu platform and, in that way, facilitating the future transfer of the website once the project is concluded.

Communication and visibility of the EU is a legal obligation for all external Actions funded by the EU.

This Action shall contain communication and visibility measures which shall be based on a specific Communication and Visibility Plan of the Action, to be elaborated at the start of implementation.

Appropriate contractual obligations shall be included in, respectively, the procurement and grant contracts, and delegation agreements.

The Communication and Visibility Manual for European Union External Action⁶, which came into force on 1 January 2018, shall be used to establish the Communication and Visibility Plan of the Action and the appropriate contractual obligations.

4 IMPLEMENTATION ARRANGEMENTS

4.1 Method of implementation

4.1.1 Procurement (direct management)

The project will be implemented through the procurement of services, either by extension of the current service contract as foreseen in AAP 2016, or by launching a call for tender. The indicative timetable for the call for tender, should this option be selected, is 3rd Quarter 2020.

The Commission will ensure that the EU appropriate rules and procedures for providing financing to third parties are respected, including review procedures, where appropriate, and compliance of the action with EU restrictive measures⁷.

---

⁷ www.sanctionsmap.eu Please note that the sanctions map is an IT tool for identifying the sanctions regimes. The source of the sanctions stems from legal acts published in the Official Journal (OJ). In case of discrepancy between the published legal acts and the updates on the website it is the OJ version that prevails.
4.2 **Indicative budget**

<table>
<thead>
<tr>
<th>Method of Implementation</th>
<th>Amount in EUR</th>
</tr>
</thead>
<tbody>
<tr>
<td>Procurement (direct management)</td>
<td>3 000 000</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>3 000 000</strong></td>
</tr>
</tbody>
</table>

4.3 **Organisational set-up and responsibilities**

The Contractor will maintain a Steering Committee with the Service for Foreign Policy Instruments and DG JUST.

This second phase will deepen the collaboration with the EEAS, the EU Delegations in partner countries and the FPI regional offices through monthly reports and clear coordination mechanisms.

4.4 **Performance monitoring**

The day-to-day technical and financial monitoring of the implementation of this Action will be a continuous process and part of the implementing entity’s responsibilities. To this end, the implementing entity shall establish a permanent internal, technical and financial monitoring system for the Action and elaborate regular progress reports (not less than annual) and final reports.

Every report shall provide an accurate account of implementation of the Action, difficulties encountered, changes introduced, as well as the degree of achievement of its results. The progress and final reports shall provide quantified and qualitative data in relation to the logical framework indicators which will include relevant indicators from the list of core and corporate indicators.

The report shall be laid out in such a way as to allow monitoring of the means envisaged and employed and of the budget details for the Action. The final report, narrative and financial, will cover the entire period of the Action implementation.

The Commission may undertake additional Action monitoring visits both through its own staff and through independent consultants recruited directly by the Commission for independent monitoring reviews (or recruited by the responsible agent contracted by the Commission for implementing such reviews).

4.5 **Evaluation and audit**

For this Action, the Commission may carry out interim and/or final/ex-post evaluation(s) via independent consultants contracted by the Commission based on specific terms of reference.

Without prejudice to the obligations applicable to contracts concluded for the implementation of this Action, the Commission may, on the basis of a risk assessment, contract independent audits or expenditure verification assignments.

As the “N+1” rule applies for contracting under this decision, external evaluations and audits, as well as additional external monitoring referred to under section 4.4. above, will be funded from sources other than those allocated to this specific Action.