Group of the Progressive Alliance of
Socialists & Democrats
in the European Parliament

European Parliament
Rue Wiertz 60
B-1047 Bruxelles
T +32 2 284 2111
F +32 2 230 6664
www.socialistsanddemocrats.eu

S&D POSITION ON DATA PROTECTION

In a world built around online communication, the modernisation of data protection laws is a pressing need for Europe. Every day our data is processed and stored in an unprecedented scale by both the private and the public sector. Our personal data has become a commodity, which value has surpassed any of our expectations. Public and private databases of sometimes highly sensitive data have cropped up and the data is exchanged within Europe as well as transferred to third countries.

The S&D Group welcomes the Commission proposal on reforming the current data protection framework and specifically welcomes that the instrument of Regulation was adopted. However, we must state our grave disappointment that the law enforcement sector was taken out of the Regulation and a Directive was chosen to cover police and judicial cooperation, as this provides and inferior level of protection to our citizens. We believe that the two instruments create a single package and that a high level of harmonisation of provisions between the two, need to be guaranteed.

The S&D Group is committed to data protection rules that protect fully our citizens' fundamental rights but at the same time encourage further harmonisation in the internal market and allow businesses to innovate, grow and create jobs.

We, the S&D, believe that the new data protection framework should be based on the following principles:

- **Territorial scope**
  - package applies to processing of personal data of data subjects **residing in the Union**, **regardless of whether the controller is a private or a public body, based in the Union or outside and regardless if the services are paid or free of charge**.

- **Definition of personal data**
  - personal data is any information that relates to a data subject
  - **anonymised** data should not be subject to the Regulation. Use of anonymised data should be encouraged and incentivised.
  - **pseudonymised** data is personal data, and the use of pseudonyms should be encouraged, and incentivised. Pseudonymisation should give some leeway from certain documentation etc. obligations

- **Principles of data processing**
  - transparency, purpose limitation, data minimisation, integrity, accountability, security and storage minimisation have to be respected

- **Lawfulness of processing**
  - processing is only legal where there is: explicit consent, compliance of a legal obligation, performance of a contract, protecting a vital interest of the data subject, processing is done by a public body for an official duty, *and in very limited and specified circumstances for legitimate interest of the controller*

- **Special categories of data**

- data revealing race or ethnicity, political opinions, religion or beliefs, trade-union membership, genetic or biometric data, sexual orientation or gender identity or data concerning health or sex life or criminal convictions is to be considered as having special protection and shall not be processed, unless in extremely specified circumstances and with special safeguards

- **Right to information, access, rectification and erasure**
  - the data subject has to have full right to be informed on and access to what data is being processed of them and for what purpose. They shall also have full rights to rectify and/or supplement the data that is incorrect and to obtain the erasure of it. The controller shall take measures to have the data erased from any third parties it has transmitted such data.
  - as a part of information policy, a system of clear icons should be used by companies on their websites, to easily show to the data subject what is being done with their data

- **Profiling**
  - every natural person shall have the right not to be subjected to profiling that would produce legal effects for the person
  - exceptions to the rule have to be specified in law or data subject's consent if that is freely given and can be withdrawn
  - profiling cannot be based on special categories of data
  - profiling cannot be used to single out children

- **One-stop-shop**
  - there has to be a one-stop-shop for both the citizen and the companies, i.e. a single contact DPA with whom to deal with when needed.

- **Transfer of data to third countries**
  - transfers to third countries should only take place when it can be guaranteed that corresponding data protection norms can be guaranteed in the country of transfer
    - COM adequacy decision, European Data Protection Seal, appropriate safeguards in a **legally binding instrument** and legally binding corporate rules
    - derogations to the above have to be necessary and proportionate in a democratic society

- **Strong Data Protection Authorities**
  - the independent national DPAs have to be guaranteed with proper resources to be able to perform their tasks
  - strong European cooperation between the national DPAs have to be ensured through the work of the EDPB and the cooperation and consistency mechanisms

- **Redress and sanctions**
  - there is a right to judicial remedy against controller or processor and against a DPA, with right to compensation and liability and penalties.
  - sanctions have to be individually determined, effective, proportionate and **dissuasive**

- **Safeguarding specific processing situations**
  - specific set of criteria is identified for processing in
    - the labour market and employment context
      - specifically to safeguard the right to collective agreements
    - the context of health
    - the context of freedom of expression
    - the context of historical, statistical and scientific research

Specifically regarding the Directive, we believe that the aforementioned principles should apply, where appropriate, and all deviations from the general rules have to be duly justified, necessary and

proportionate in a democratic society, clearly demarcated and set in law. Such limitations can only be an exception to the general rule and cannot become the rule itself - therefore no blanket exceptions can be accepted.