Information Notice – Read Carefully

Capgemini Data Protection Approach through Binding Corporate Rules

- **Capgemini** in the course of delivering IT consulting, technology and outsourcing services to clients and other Capgemini affiliates, accesses regularly personal data (personally identifiable information) including in some cases, sensitive personal data.

  - **Examples of Personal Data:** *Contact data: Name, Address, Telephone nos., Email id. Identification data: Gender, ID Cards, Date & Place of Birth, Govt Id., Passport, Driver's License Work/Payroll data: compensation, benefits, qualifications, work history, employee id; Business Contact Information, etc.*
  - **Examples of Sensitive Personal Data:** *Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership (photos, films, etc.); Data concerning health or sex life, medical records, criminal records - Medical data, health reports, biometrics, court records; Data relating to the finances/financial situation - Debt, salary, payment data, bank account, credit / debit card number, CVV number, Pan Card No.; Data relating to Insurance records - Insurance Payments, Insurance Nos., etc.*

  - Most countries (and not only in the European Union (EU)) the processing of personal data is strictly regulated. Capgemini is committed to comply with these Rules. Our clients expect us to provide a high level of protection to the personal data we process on their behalf irrelevant of the place from which Capgemini process and/or access such personal data.

  - To address this client expectation and to ensure compliance with applicable data protection regulations, Capgemini has adopted Binding Corporate Rules (BCR). These BCR constitute the Group's common data protection Policy laying down the principles with which each Capgemini entity and its employees shall commit to comply with. It sets the framework for uniform levels of protection, security standards and practices in handling personal data by all Capgemini entities across the globe.

- **Every Employee must be aware of the BCRs and must read them– You can find Capgemini by clicking here.**

In a nutshell, what do the BCRs Encompass:

- The BCRs describe & explain the data protection principles both, when we process: (i) Capgemini employee data (as a Data Controller) & (ii) Our Client's employee, customer, or vendor data (as a Data Processor). Capgemini must comply with Client instructions. **This means, as agreed with the Client & where technically possible:**
  - Consult the description of the engagement in e-Monitoring and in eMMX and make sure you have the answers to the following questions:
    - ✓ What am I allowed to do with the personal data according to client's instructions?
    - ✓ After which period of time shall I delete the personal data?
    - ✓ With which entity can I share and/or make accessible the personal data?

- Process the personal data only for the purposes for which their collection/processing was initially defined;
- Don't try to collect/process personal data which have not been expressly defined by the client and which are not strictly necessary;
- Be aware of and understand the client's instructions;
- Ensure that the technical and organizational measures necessary for the project are well implemented;
- Ensure that the personal data are deleted and/or returned according to client's instructions, in particular when the engagement ends;
- Ensure that appropriate technical measures are in place to be able to retrieve and/or amend personal data according to clients' instructions.

- As a Data Processor, Capgemini is committed to process personal data in compliance with client instructions & legal requirements. Capgemini must support Client to enable Client's compliance with data protection laws. **This means**:
  - *Engagement/Delivery Managers must ensure flow down of all data protection & Security requirements agreed with Client, to the Team.*

- Capgemini must implement "appropriate" security controls as agreed with the client for provision of services or while designing a solution. **This means**:
  - *Capgemini must notify the Client of any data breaches, & assist Client in addressing the breach, as per Capgemini incident management procedures & escalation process.*
  - *Support the Client in implementing reinforced security measures in processing sensitive data.*
  - *Every employee shall act with care while processing personal data.*
  - *Every employee must adhere & respect client's security controls, policies, firewalls & never breach the same*.
  - *Every employee needs to understand and comply with the physical, logical, network and security controls on the project and be alert to any vulnerability/exposure.*

- Each employee shall follow the mandatory data protection training and shall attend any specific data protection training that he/she will be offered to attend.

- The implementation of the BCR rely on a strong network of data protection officers (DPO) at group, regional & local levels working with privacy champions within the BU's & functions. You must be aware of the DPO organization. **Please reach out to your Local Data Protection Officer for details or any questions regarding this Information notification. Click here to find out who is the Local Data Protection Officer you should reach out to.**

Capgemini Group Data Protection Officer