Een ruimte waarin gewerkt wordt met **Wet politiegegevens (Wpg)**-gegevens moet voldoen aan strikte eisen op het gebied van **beveiliging, toegang, en privacybescherming**. Deze wet stelt regels aan hoe politie en opsporingsdiensten met persoonsgegevens om moeten gaan, met als doel de privacy van burgers te waarborgen.

Hieronder de belangrijkste eisen waaraan de werkruimte moet voldoen:

🔐 Fysieke beveiliging van de ruimte

- **Toegangscontrole**: Alleen geautoriseerde medewerkers mogen toegang hebben tot de ruimte. Toegang moet beperkt en controleerbaar zijn (bijv. via pasjes of sleutels met logging).
- **Afgesloten ruimte**: De werkplek moet zich in een afsluitbare ruimte bevinden (geen open kantoorvloer), die niet zomaar toegankelijk is voor derden.
- **Beveiliging tegen inbraak en brand**: Denk aan gecertificeerde sloten, alarmsystemen, rookmelders, brandblussers.

💻 Technische beveiliging

- **Versleuteling**: Gegevensdragers (laptops, USB-sticks) met politiegegevens moeten versleuteld zijn.
- **Beveiligde netwerken**: Alleen via beveiligde verbindingen (VPN, firewalls) toegang tot systemen waarin politiegegevens verwerkt worden.
- **Beperking van kopieën**: Opslag van gegevens moet zo veel mogelijk centraal gebeuren. Vermijd lokale kopieën.
- **Logging en monitoring**: Het gebruik van politiegegevens moet gelogd worden. Wie wat bekijkt of bewerkt moet herleidbaar zijn.

🕵️ Toegang en bevoegdheden

- **Autorisatiebeheer**: Alleen medewerkers met een specifieke, aantoonbare rol mogen toegang hebben tot de gegevens.
- **Screening personeel**: In veel gevallen moeten medewerkers een veiligheidsonderzoek ondergaan.
- **Bewustwording & training**: Medewerkers moeten getraind zijn in de Wpg en informatiebeveiliging.

📋 Procedureel en organisatorisch

- **Verwerkersovereenkomsten**: Als derden betrokken zijn bij verwerking (bv. een IT-leverancier), moet dit contractueel goed zijn vastgelegd.

- **Beveiligingsbeleid**: Organisaties moeten een informatiebeveiligingsbeleid hebben dat voldoet aan de normen (bv. BIO of ISO 27001).
- **Audit en toezicht**: De Autoriteit Persoonsgegevens en Inspectie Justitie en Veiligheid mogen audits uitvoeren.

📘 Relevante artikelen uit de Wpg

🔐 1. Beveiliging van politiegegevens

Artikel 33 Wpg – Beveiliging van verwerking

- Verplichting voor de verantwoordelijke om passende technische en organisatorische maatregelen te nemen ter beveiliging van de gegevens.
- Gericht op bescherming tegen verlies, onrechtmatige verwerking, onbevoegde toegang, en wijziging.

➡️ Dekt:

- Fysieke beveiliging van de ruimte
- Versleuteling
- Netwerkbeveiliging
- Autorisatiebeheer

🕵️ 2. Beperking van toegang en autorisaties

Artikel 34 Wpg – Toegang op basis van autorisatie

- Alleen personen die daartoe zijn gemachtigd mogen toegang hebben tot politiegegevens, voor zover noodzakelijk voor hun taakuitvoering.

➡️ Dekt:

- Toegangscontrole
- Autorisatiebeheer
- Rollen en rechten
- Geen onbeperkte toegang

💻 3. Logging en controle

Artikel 35 Wpg – Logging en controlemaatregelen

- De verwerking van politiegegevens moet gelogd worden.
- Doel: controle op rechtmatigheid van toegang en verwerking.

- Logs moeten bewaard worden en mogen alleen worden ingezien door daarvoor aangewezen personen.

➡️ Dekt:

- Logging en monitoring
- Controle op wie wat doet met gegevens

👨‍💼 4. Verwerkers en derden

Artikel 36 Wpg – Verwerking door derden (bewerkers)

- Als een externe partij betrokken is bij de verwerking, moet dit contractueel vastgelegd zijn.
- De externe partij moet ook voldoen aan de beveiligingseisen.

➡️ Dekt:

- Verwerkersovereenkomsten
- Verwerking door derden (zoals IT-leveranciers)

🏢 5. Interne procedures en toezicht

Artikel 37 Wpg – Interne controle en evaluatie

- Periodieke toetsing van de verwerking en beveiligingsmaatregelen.
- Verantwoordelijke moet interne controles uitvoeren.

➡️ Dekt:

- Audits
- Interne beveiligingsprocedures
- Beleid en evaluatie

👮 6. Toezicht door autoriteiten

Artikel 38 t/m 40 Wpg – Toezicht en handhaving

- Inspectie Justitie en Veiligheid houdt toezicht op naleving.
- Sancties mogelijk bij overtreding van de wet.

➡️ Dekt:

- Externe controle (Inspectie JenV)
- Verantwoording en handhaving