Differential Privacy

Original Data $+$ Calibrated Noise 🔒 $=$ Protected Data 🔒

Mechanisms

Gaussian Mechanism

Laplace Mechanism

Privacy Budget (ε)

ε remaining

Parameters

ε
Privacy Loss
Lower = More Private

δ
Failure Probability
Typically 10^{-5}

Typical Values
$\varepsilon = 1\text{-}10$
$\delta = 10^{-5}$