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
ε = 1-10
δ = 10^{-5}